

Active Directory Single Sign-on For IV&C Servers

Revisions

July 12, 2006	O. Jones	First Release
July 14, 2006	O. Jones	Minor editorial corrections

Abstract

You can deploy IV&C's viewer-controlled video across your enterprise. In an enterprise environment, your computer users need appropriate access to video resources. This white paper explains how IV&C's customers can use a Windows Domain Controller based on Microsoft Active Directory to provide central user authentication and access control for IV&C's Relay Server Software.

The intended audience for the executive summary of this white paper is the information technology manager and enterprise security manager. For the detailed discussion, the intended audience is the Domain Administrator and the Video Administrator. This documentation assumes that the Domain Administrator is familiar with the mechanics of maintaining security groups and users in the domain.

The integration between IV&C and the directory server is designed to allow your existing Windows domain infrastructure to provide single sign-on for IV&C's viewer-controlled video. Domain Administrators may grant selected users access to IV&C servers, and grant each user appropriate access rights. These grants of access and rights may be given to individual named users and, at the customer's option, to groups.

Use of a Windows Domain Controller is not required to deploy video services. IV&C customers may choose to use other means of granting users access. IV&C offers integration with LDAP enterprise directories, as well as stand-alone authentication and access control. These other methods of authentication and access control are described in other documents.

Executive Summary

With single-sign-on, any authorized user in a Windows Domain may access IV&C viewer-controlled video. For example, any authorized user of a regional public safety network can gain appropriate access to video servers.

Some users need to see video. Others need to control the positioning of cameras. A few users need to manage the operation of the video cameras, or administer video servers. Using IV&C's single-sign-on administration, it becomes simple and cost-effective to plan and implement a coherent enterprise-wide video policy.

Users may be assigned access permissions in groups or individually. For example, a certain group of users might be granted permission simply to see video. Other users might be granted permission to view and control the cameras, and to record video clips. Still others might have the additional permission to set up preset views. This allows a viewer-controlled video administrator easily to grant, and to revoke if necessary, appropriate access to each constituency.

Granting of access permission is handled through the Domain Controller, in the same way that access is granted to other information technology resources. Therefore, this solution is cost-effective, scalable, and easily auditable for both small-scale and large-scale operations.

Planning and Operational Responsibilities

An hour or two spent planning for enterprise video deployment will yield long-term benefits. The enterprise domain administrator and the person responsible for video deployment should meet to plan for the video system deployment.

The domain administrator must perform some one-time Domain Controller configuration work when the first IV&C Relay Server Software is installed in the enterprise, and some more work when each new Relay Server is installed. IV&C furnishes a utility program to do this work.

The domain administrator or a delegate must grant permissions to individual users or groups. Access can be added or revoked at any time at the domain administrator's option. This work must be done using the Active Directory Users and Computers utility or the equivalent.

The computer administrator responsible for installing each IV&C Relay Server must do some one-time installation work on each server to connect it to the Domain Controller, and briefly requires assistance from the Domain Administrator.

When new users are added into the Domain Controller, it will be necessary for the person creating their accounts to grant them appropriate access to video resources. Additionally, each user must run a video-access client program before accessing IV&C's Relay Server Software. Once the video-access client program is running, the operation of the system is transparent to end-users. Once a user is logged in to a computer that is a member of the enterprise domain, that user's access to video is based on that user's identity.

Controlling Enterprise Video Access Permissions

Users of enterprise viewer-controlled video may be granted blanket permission – to see video, to control cameras by pointing them at anything in their field of view, and to create and delete archival video footage. Or, at the option of the system administrator, viewers

may be granted fewer permissions, restricting them to using features they need to do their jobs.

The IV&C Relay Server Software offers a variety of operations to the end user who uses a web browser or the IV&C View Station software to carry them out. Each of these operations has a particular Permission accompanying it. The Permissions and Operations available in the Relay Server Software appear in the table. Each permission may be granted to appropriate users or groups of users.

Name of Permission	Relay Server Software Operation
Relay Server View	View video feeds
Relay Server Archival Create	Create video clips stored in archives
Relay Server Archival Delete	Delete video clips from archives
Relay Server Manage	Set up preset positions and panoramas
Relay Server Camera Control	Control what cameras see by causing them to pan, tilt, and zoom
Relay Server Administrate	Administer Relay Servers

Planning Enterprise Video Deployment

If you invest a modest amount of time in up-front planning for your video deployment you will be able to create an easily maintainable enterprise-wide video system.

A good way to grant users appropriate access to the video system is to group them by the kind of access they need. Windows Domain Controller allows your domain administrator to create Security Groups. These groups are an ideal way to organize access to IV&C's viewer-controlled video. Some organizations may find that they already have already classified their users into appropriate Security Groups, and others will find that they need to create new ones specifically for video deployment.

When you plan for enterprise deployment of viewer-controlled video, you will find it helpful to consider five areas of access: Content, Control, Archiving, Management, and Administration.

Content describes the live images your users can see on the installed video cameras. It also describes what they can see in the stored archives of video and snapshots. When you plan for enterprise access to video content, decide which of your users have a need for particular content.

Are any of your video cameras positioned in such a way that access to the live images must be carefully restricted? An example might be cameras that monitor proprietary production processes. If the content from certain cameras is highly sensitive, it is probably best to deploy those cameras through a separate Relay Server, and restrict access to that Relay Server.

The basic question is, “who needs to see the video feeds?” Planning for video deployment must answer that question. Some installations will opt for a need-to-see policy, while others will choose a more open approach.

If you adopt the need-to-see policy, you will do well to create a Group in your Windows Domain Controller with a name like “Video Viewers,” and grant “Relay Server View” permission to that group. You will then grant access to the video system by making the appropriate users members of that group. Another possibility is to use an existing group (a “Corporate Security” group might be an example), and grant permission to that group.

If you adopt a wide-open policy you might choose to grant the “Relay Server View” permission to the pre-existing “Domain Users” group in your Windows Domain Controller, or to another group most users already belong to.

Control refers to the capability of your users to pan, tilt, or zoom video cameras in the viewer-controlled video environment. IV&C offers a variety of cameras that users can pan, tilt, and/or zoom. Some organizations will permit everyone who needs to see video also to control camera positions. For example, if your video installation monitors a production process, your video users will need to zoom in on a particular part of the process to take a closer look. You can implement this kind of policy by granting “Relay Server Camera Control” permission to the “Video Viewers” group, the same group that lets your users see the video.

Other organizations will restrict control to certain users. For example, in a highway monitoring application it might be helpful to grant control permission only to public safety specialists. That way they can do their jobs in emergency situations without having other users – “rubbernecks” – seize control of the cameras just for the sake of curiosity. You can implement this kind of policy by creating a group named, for example, “Video Controllers,” and granting both the “Relay Server Camera Control” and “Relay Server View” permissions to it. Include in this group your users whose jobs require them to view and control cameras.

Archiving refers to the storage of snapshots and video in the Relay Server. Anyone with permission to view live video can also view video archives and snapshots.

Do you need archives of the video feeds? Some installations require continuous archiving of video feeds, and others need on-demand archiving. Some may use both, in order to keep both continuous records and records of particular events.

Your video administrator sets up continuous archiving of video streams when configuring the Relay Server Software to access each new camera (using the “Relay Server Administrate” permission described later in this section). Once you have set up

continuous archiving, your users need not be concerned with its management; it reclaims the oldest archive storage automatically so it can operate continuously.

If your application needs on-demand video archiving or snapshot creation, it is wise to decide which users may initiate the creation of an archive. Grant the “Relay Server Archival Create” permission to any group (or individual user) who needs to initiate the creation of these archives.

You also may decide which users, if any, have permission to delete stored archives and snapshots. If your application involves a large number of user-initiated snapshots or archives are created, you may find manual deleting to be helpful. Grant the “Relay Server Archival Delete” permission to any group of users (or individual user) who needs to delete snapshots or archives manually.

Keep in mind that the IV&C Relay Server Software automatically deletes the oldest video archives and snapshots in your server when it needs to reclaim hard-drive space so that archiving can continue. You do not need to grant any specific permissions to users for the Relay Server Software’s automatic space-reclamation function to work correctly.

Is it important for your application to prevent users from deleting specific stored video archives or snapshots? This is true for many security applications. To make sure that nobody deletes particular segments of the video archives, withhold this permission from all users. In this case both archives and snapshots will remain available until they become old enough to be deleted automatically when the Relay Server Software needs to reclaim hard-drive space.

Notice also that the “Relay Server Archival Delete” permission only controls access to archives via IV&C’s Relay Server Software. A user who has access to the Relay Server’s file system via direct access to the server’s host computer or via a file share can always delete some or all archive and snapshot files.

Management of viewer-controlled video is IV&C’s name for the work of aiming the cameras: of setting up preset pan-tilt-zoom positions and panoramas. Any user or group of users who must do this work needs the “Relay Server Manage” permission. In some cases, it may be helpful to allow all video users to do this. For example, video users who monitor a production process may choose to add new preset positions focusing on particular areas of interest. In this case, these users’ group should be granted “Relay Server Manage” permission. Other installations may prefer that only certain users do this work.

Administration of viewer-controlled video is the work of setting up the Relay Server Software, configuring it to control its use of storage and of network bandwidth, and enabling it to access new cameras. Any user or group of users who must do this work

needs “Relay Server Administrate” permission. You should avoid granting this permission to casual video users

We suggest you create a security group in the Windows Domain Controller called “Video Administrators,” and grant all Relay Server permissions (except possibly “Relay Server Archival Delete”) to that group. Then you can add a limited number of your users – the people who need to administer the video application – to that group.

Summary

Successful deployment planning will produce answers to the following questions.

- Which users need to see the video content? What security group or groups will they be in?
- Do all your users who need to see video also need to control camera pan-tilt-zoom positions? If not, which security group or groups will you use to grant permission to them to pan, tilt, and zoom the video cameras?
- Which users, if any, need to create video archives? Do any users need the ability to delete them? What security groups will you use to grant this access?
- Which users need permission to aim the cameras at preset positions? What security groups will you use to grant this access?
- Can you use the security groups already existing in your organization’s Domain Controller to grant access to video? If not, what new security groups will you create?
- Who will administer your Relay Server Software? We suggest that you create a Video Administrators security group to control administrative access to the Relay Server Software.
- Who will configure your Domain Controller to support the IV&C Relay Server Software as it is installed? This person needs to be a Domain Administrator. We provide a utility program to help you do this.
- Who will responsible for ongoing configuration of the video deployment in your Domain Controller, adding any required security groups and adding users to those groups? This person needs to be a Domain Administrator or someone to whom the Domain Administrator has delegated appropriate access.
- How sensitive is your application to unauthorized deletion of video archives? If you are sensitive to this, how will you restrict access to the physical hardware and file systems of the computers running the Relay Server Software? We suggest you avoid creating file shares on the Relay Server Software computer unless your application requires it.

Once you know the answers to these planning questions, you can proceed to configure your Domain Controller, install your Relay Server Software, and use the Active Directory Users and Computers utility (it is actually a Microsoft Management Console snap-in) to grant access.

Domain Administrator Deployment Tasks

IV&C's Relay Server Software integrates with the Active Directory software in your Domain Controller. We use it to authenticate users, and to store the rights you grant each user to access video services. This section of the white paper is intended for a Domain Administrator familiar with Active Directory. We assume you know how to use the Active Directory Users and Computers (ADUC) utility (a snap-in for the Microsoft Management Console) to add Security Groups to your domain and to put your users into those groups.

As a Domain Administrator you will perform the following tasks to deploy our software in your domain.

1. Participate in planning your video deployment.
2. Configure your Domain Controller, just once.
3. Configure each computer server that will run our Relay Server Software, and install our software on it.
4. Create appropriate Security Groups and assign users to them.
5. In your Domain Controller, assign appropriate IV&C permissions to your security groups and users.
6. Configure each user workstation.

The next sections of this document give specific instructions for these steps.

The ongoing maintenance you must do as a Domain Administrator for your IV&C video deployment is modest.

1. When you create new user accounts, you will need to put them into appropriate groups to grant them video access.
2. From time to time you may need to add particular users to or remove them from your video security groups as their job responsibilities change.

One-time Domain Controller Configuration

To prepare your Domain Controller to support single-sign-on for IV&C's Relay Server Software, you must load our "controlAccessRight" objects. These provide the custom permissions our software needs. To load these objects into the Domain Controller, use the console-mode application we furnish called EnsecConsole.exe. You need to use this application while logged in as a domain administrator. You can run it on the domain controller, the Relay Server Software machine, or a workstation – as long as you run it when logged in as a Domain Administrator.

Type the following commands in a command console window. Boldface indicates what you should type. The **fi** (forest install) command loads our objects into the Active Directory forest. The **fc** (forest check) command verifies that they are loaded correctly.

```
C:\> cd \IVC
C:\IVC> EnsecConsole
```

```
. . . .
Client console
-----
Type 'help' for commands

> fi
Connecting to directory services...
Connected to domain (DC=myorganization,DC=com)

Forest installation successful.

> fc

Application INSTALLED on forest.

> exit
C:\IVC>
```

Relay Server Software machine configuration

We strongly recommend that you dedicate a computer to running the Relay Server Software. To run the Relay Server Software with Active Directory single-sign-on enabled, you must provide the following environment.

- 1) The server computer must be a member of the domain.
- 2) The domain account you use to run the Relay Server Software must have local administrator rights. (It should not be a Domain Administrator, however.) To set this up, log into the machine as a local administrator, then go to Control Panels / User Accounts. Click Add, then give the domain name and account name. Click Next>, then grant Administrator access to the user, as follows, and click Finish.



- 3) Avoid making file shares available from the Relay Server Software server computer if at all possible. If you must make file shares available, make sure they are properly secured.

Next, log in to the account you will use to run the Relay Server Software. Install, but do not yet run, the Relay Server Software.

Finally, log in to the Relay Server machine, just once, using a Domain Administrator account. Type the following commands in a command console window. Boldface indicates what you should type. The **si** (server install) command sets up the server machine in Active Directory to run the Relay Server Software. It adds a custom serviceConnectionPoint object called “IVCRelayServer” to the Active Directory entry for the computer it is running on.

```
C:\> cd \IVC
C:\IVC> EnsecConsole
. . .
Client console
-----
Type 'help' for commands

> si

Server installation successful.

Service ID = 24f1b694-4041-49e4-b644-6b486189dbe3
Service DN = CN=IVCRelayServer,CN=MYCOMPUTER,CN=Computers,DC=myorganization,
DC=com

> exit
```

Adding Domain Security Groups and Users

Use the Active Directory Users and Computers tool (ADUC) to create the necessary security groups for your video application deployment, and assign your users to those groups as required.

PLEASE NOTE: In “mixed mode” Active Directory deployments (containing features for access by pre-Windows-2000 computers), Security Groups you use to control access to video services must have “Global” or “Universal” scope. Groups with “Domain local” scope do not work for this purpose.

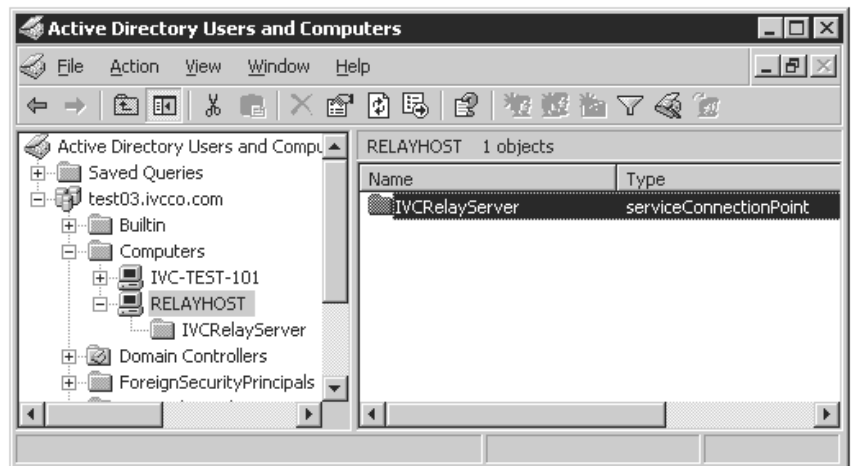
Granting Video Permissions to Groups and Users

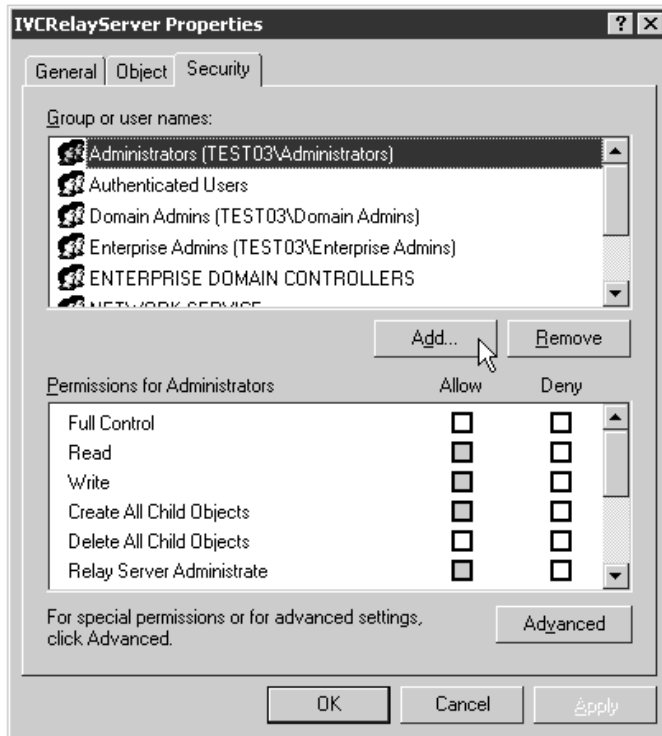
When you have created the appropriate Security Groups, you are ready to grant video-specific access permissions to those groups, as well as to any particular users who need access. Use ADUC for this. These instructions cover the use of the version of ADUC that ships with Windows Server 2003.



Before you start trying to grant permissions, start up ADUC and enable its advanced features. On the View menu, make sure there are check marks next to “Users, Groups and Computers as containers,” and to “Advanced Features,” as shown here.

Next, locate the computer that will be running the Relay Server Software in the ADUC tree display. You will find it under Computers. In this example it is called “RELAYHOST.” Nested underneath the computer locate the serviceConnectionPoint called IVCRelayServer and click on it.

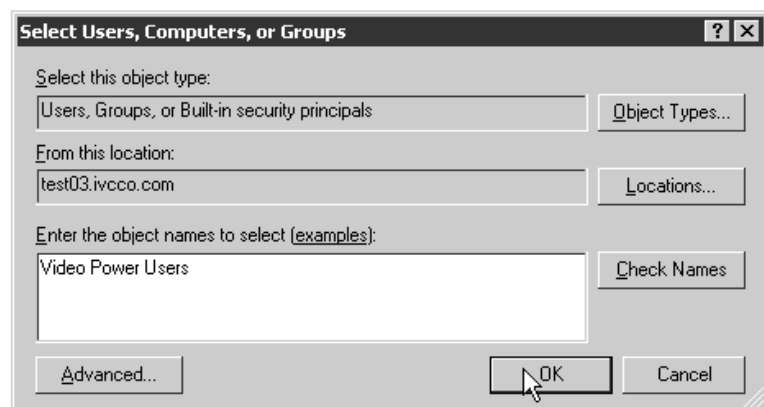




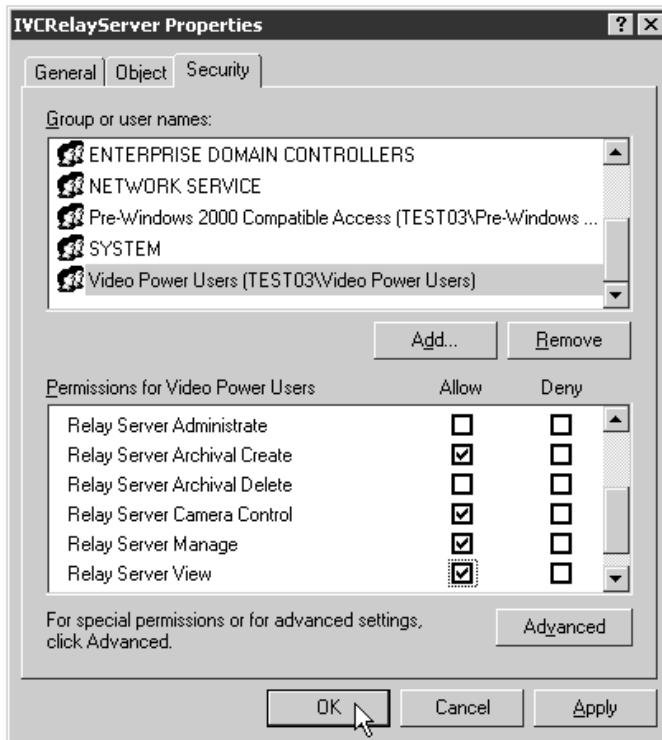
Click on the Action menu, choose the Properties ... item, then click on the Security tab of the properties window. The IVCRelayServer security tab looks like this.

PLEASE NOTE: If ADUC does not show the IVCRelayServer item associated with your Relay Server computer, make sure you have correctly configured it using our EnsecConsole utility program, and also that you have enabled ADUC's advanced features of ADUC. If ADUC does not show Security tab, make sure you have enabled its advanced features.

Now, you are ready to grant permissions to security groups and users. Click on the Add... button, enter the name of a security group or a particular user, and click OK. This example assumes you have already created a Security Group called "Video Power Users" and are now granting permissions to that group.



The Security tab returns. Make sure the name of the group you just added is highlighted, and scroll down under Permissions so you can see the Relay Server permissions. Choose the appropriate permissions by clicking in the boxes under Allow, then click Apply. In



this example, you are granting permission to create archives, to manage the cameras, to control them, and to view video. Notice that you do not have to check Deny for the other permissions. (If you do choose to Deny particular permissions, please make sure you understand how Deny entries work in Windows Access Control Lists. A discussion of that topic is beyond the scope of this document.)

Repeat this operation to grant permissions to each security group you created, and to any particular named users who need their own permissions.

User Workstation Configuration

Each user must run the program named “ensecClient.exe” before attempting to access video resources via web browsers or the IV&C View Station software package. For user convenience, you (the administrator) should copy this program from the C:\IVC folder on the machine running the Relay Server Software to each user’s desktop, and instruct the user to run the program before accessing video resources.

Video Administrator Deployment Tasks

This document describes the tasks you must carry out as Video Administrator to deploy IV&C’s single sign-on in your enterprise. You must also configure the Relay Server Software for correct operation. The details of that configuration are described in other documents.

Starting up the Relay Server Software

Log in using the account your Domain Administrator created to run the Relay Software, and start it up. To run a Relay Server using Active Directory authentication and access control the following command line is required:

```
ivc-relay -authentMode 1
```

You may store and change command line parameters by creating a Windows Shortcut to run the Relay Server Software and editing its properties.

Once you have started up the Relay Server Software, you may use an Internet Explorer web browser to access it and configure it.

Testing and Troubleshooting

Make sure the Domain Administrator has assigned a user to an appropriate Security Group granting access to the Relay Server Software. Then, log in to a domain workstation using that user's account. Run the IV&C-furnished authentication utility called EnsecClient. Bring up an Internet Explorer web browser, and enter the URL of the Relay Server Software. Try various operations. When permissions are not available, you should get a dialog box, similar to the one shown here, describing the problem.



The text "Video Temporarily Down" in the video window on your user's Internet Explorer window indicates that your user does not have the "Relay Server View" permission necessary to see the video content. (This message also can indicate that something is wrong with the video camera.)

If your user seems to have access to permissions that you did not grant, ensure that you ran the Relay Server Software using the `-authentMode 1` command line parameter.

PLEASE NOTE: A web browser running on the same computer as the Relay Server is useless for testing whether Relay Server Software access permissions are configured correctly. This is because the Relay Server Software automatically grants all permissions to local web browsers.