



**CITADEL**<sup>TM</sup>  
SECURITY SOFTWARE

**CITADEL**  
**Hercules**<sup>TM</sup>  
Automated Network Vulnerability Remediation

Hercules Security Configuration Guide





**Citadel™ Security Software Inc.**

**Hercules® Security Configuration Guide**

Document No. 205-01-0011

Hercules v3.5.0

Document Version 1.0

December 2004

## Acknowledgements

THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR DOCUMENTATION.

The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to the software without specific, written prior permission. Title to copyright in this software and any associated documentation will at all times remain with copyright holders.

Citadel and ConnectGuard are trademarks of Citadel Security Software Inc. Hercules is a registered trademark of Citadel Security Software Inc. Hercules software is copyrighted by Citadel Security Software Inc. Hercules software is a patent-pending Automated Vulnerability solution. Active Directory, Microsoft, Windows, Windows Server, Windows NT, and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Internet Scanner, System Scanner, and SiteProtector are trademarks or registered trademarks of Internet Security Systems. Foundstone and FoundScan are trademarks of Foundstone, Inc. STAT is a registered trademark of Harris Corporation. QualysGuard and Qualys are trademarks of Qualys, Inc. Retina is a registered trademark of eEye Digital Security. SecureScout SP is a trademark of NexantiS Corporation. SAINT is a registered trademark of the Saint Corporation. Linux is a registered trademark of Linus Torvalds. Red Hat is a registered trademark of Red Hat, Inc. Sun and Solaris are trademarks of Sun Microsystems, Inc. UNIX is a registered trademark of The Open Group. AIX is a registered trademark of International Business Machines Corporation. Mac OS X is a registered trademark of Apple Computer, Inc. HP-UX is a registered trademark of Hewlett Packard Company in the United States. Apache is a trademark of the Apache Software Foundation.

### W3C® SOFTWARE NOTICE AND LICENSE

Copyright © 1994-2004 World Wide Web Consortium <http://www.w3.org/>, (Massachusetts Institute of Technology <http://www.lcs.mit.edu/>, Institut National de Recherche en Informatique et en Automatique <<http://www.inria.fr/>>, Keio University <<http://www.keio.ac.jp/>>). All Rights Reserved.

<http://www.w3.org/Consortium/Legal/>

This W3C work (including software, documents, or other related items) is being provided by the copyright holders under the following license. By obtaining, using and/or copying this work, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions:

Permission to use, copy, modify, and distribute this software and its documentation, with or without modification, for any purpose and without fee or royalty is hereby granted, provided that you include the following on ALL copies of the software and documentation or portions thereof, including modifications, that you make.

The full text of this NOTICE in a location viewable to users of the redistributed or derivative work.

Any pre-existing intellectual property disclaimers, notices, or terms and conditions. If none exist, a short notice of the following form (hypertext is preferred, text is permitted) should be used within the body of any redistributed or derivative code: "Copyright © 2004 World Wide Web Consortium <http://www.w3.org/>, (Massachusetts Institute of Technology <http://www.lcs.mit.edu/>, Institut National de Recherche en Informatique et en Automatique <http://www.inria.fr/>, Keio University <http://www.keio.ac.jp/>). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>"

Notice of any changes or modifications to the W3C files, including the date changes were made. (We recommend you provide URIs to the location from which the code is derived.)

All other products are trademarks of their respective holders.

Copyright © 2003-2004 by Citadel Security Software Inc. All rights reserved. This document cannot, in whole or part, be copied, photographed, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written consent from Citadel Security Software Inc.

---

# Contents

---

<b>1. Hercules® Security Recommendations .....</b>	<b>1-1</b>
Introduction .....	1-1
Assumptions .....	1-1
Securing Hercules .....	1-1
Hercules Architecture .....	1-2
Configuration Recommendations for Hercules Server .....	1-3
Hercules Security Levels .....	1-3
Update Patches and Hot Fixes on all Types of Hercules Servers .....	1-3
Level 1 - Baseline Security Configuration .....	1-3
Internet Information Services Lockdown .....	1-3
Basic Shutdown of Unnecessary Services .....	1-3
Securing Hercules Channel Server and Download Server Web Pages .....	1-4
Allowing Sudo Access for Hercules Servers and Devices .....	1-4
Basic Microsoft SQL Server 2000 Desktop Engine Configurations .....	1-4
Basic Microsoft SQL Server 2000 Configurations .....	1-4
Basic Auditing .....	1-4
Level 2 - Moderate Security Configuration .....	1-4
Moderate Shutdown of Unnecessary Services .....	1-4
Directory and User Security .....	1-5
Configuring SSL .....	1-5
Moderate Microsoft SQL Server 2000 Desktop Engine Configurations .....	1-5
Moderate Auditing .....	1-5
Role-Based Authorization .....	1-5
Enforce the Security Patches and Level 1 or Level 2 Configuration Policies .....	1-6
Securing the Microsoft Data Engine (MSDE) .....	1-9
Hercules Databases .....	1-9
MSDE Level 1 Security Recommendation .....	1-9
MSDE Level 2 Security Recommendation .....	1-9
<b>2. Securing Microsoft® IIS for Hercules® .....</b>	<b>2-1</b>
Secure Microsoft Internet Information Services 5.0 for Hercules .....	2-1
<b>3. Securing Hercules® Folders &amp; Files .....</b>	<b>3-1</b>
Securing Directories and Files for Hercules Server .....	3-1
Restricting User and Group Access to Any Type of Hercules Server .....	3-1
Restrict User and Group Access in Windows 2000 .....	3-1
Restrict User and Group Access in Windows 2003 .....	3-3

- Restricting Access to Hercules Working Directories ..... 3-4
  - Restrict Access to Hercules Working Directory in Windows 2000 ..... 3-4
  - Restrict Access to Hercules Working Directory in Windows 2003 ..... 3-6
- Restricting Access to Hercules Databases ..... 3-10
  - Restrict Access to Hercules Databases in Windows 2000 ..... 3-10
  - Restrict Access to Hercules Database in Windows 2003 ..... 3-12
- 4. Configuring SSL in Hercules® System ..... 4-1**
- Using SSL and Certificates in the Hercules System ..... 4-1
  - Using SSL and Certificates ..... 4-1
  - Public and Private Key Certificates and Certificate Authority ..... 4-1
  - Certificate Types ..... 4-1
  - Hercules Server and Hercules Download Server Certificates ..... 4-1
  - Hercules Client Certificates ..... 4-2
  - Certificate Authority ..... 4-2
  - Preparing to Configure SSL in Hercules Servers ..... 4-2
    - Enable SSL and HTTPS for Clients for UNIX, Linux and Mac OS X ..... 4-2
    - Configure 128-bit Encryption in Hercules Clients ..... 4-2
    - Uninstall Hercules Clients for Microsoft Windows ..... 4-3
- Configuring SSL in Hercules System Using Localhost Mode ..... 4-4
  - Configuring Hercules to Use Certificates With 1-Way Authentication ..... 4-4
    - Overview of Setting Up SSL and Certificates in Hercules (1-Way) ..... 4-4
    - Requesting and Installing CA Certificates on the Hercules Server (1-Way) ..... 4-5
    - Retrieve and Install the CA Root Certificate for Clients for Windows ..... 4-5
    - Configure Hercules Clients for UNIX to use CA Root Certificate (1-Way) ..... 4-5
    - Configure the Hercules Administrator to use SSL (1-Way only) ..... 4-6
    - Configure Server URLs to Use HTTPS (1-Way) ..... 4-6
    - Configure HTTPS Communications to Work with CMS (1-Way only) ..... 4-8
    - Modify Hercules Server URL from HTTP to HTTPS in hclient.conf ..... 4-10
    - Configure IIS to Require SSL Access (1-Way) ..... 4-11
    - Reinstall Hercules Clients for Microsoft Windows (1-Way) ..... 4-12
    - Restart Hercules Clients for UNIX, Linux, and Mac OS X ..... 4-13
  - Configuring Hercules to Use Certificates With 2-Way Authentication ..... 4-14
    - Overview of Setting Up SSL and Certificates in Hercules (2-Way) ..... 4-14
    - Requesting and Installing CA Certificates on the Hercules Server (2-Way) ..... 4-15
    - Configure Hercules Clients for Microsoft Windows to use SSL (2-Way) ..... 4-15
    - Configure Hercules Clients for UNIX to use CA Certificates (2-Way) ..... 4-16
    - Configure Hercules URLs to Use HTTPS (2-Way) ..... 4-16
    - Configure Clients for UNIX, Linux, and Mac OS X to Use HTTPS (2-Way) ..... 4-16
    - Configure IIS to Require SSL Access and CA Client Certificates (2-Way) ..... 4-17
    - Restart Hercules Clients for UNIX, Linux, and Mac OS X ..... 4-17
    - Reinstall Hercules Clients for Microsoft Windows (2-Way) ..... 4-18
- Configuring SSL in Distributed Hercules Architecture ..... 4-19
  - One-Way Authentication in Hercules ..... 4-19

---

Two-Way Authentication in Hercules .....	4-20
<b>5. Auditing All Hercules® Servers .....</b>	<b>5-1</b>
Setting up Audit Logging in Microsoft Windows .....	5-1
Microsoft TechNet and Help Resources .....	5-1
Preventing Audit Trail Overflow .....	5-2
Prevent Audit Trail Overflow in Windows Server 2000 .....	5-2
Prevent Audit Trail Overflow in Windows 2003 Server .....	5-4
Auditing All Types of Hercules Servers .....	5-7
Configuring Microsoft Internet Information Services Audit Logging .....	5-7
Configure IIS 5.0 Audit Logging in Windows 2000 Server .....	5-7
Configure IIS 6.0 Audit Logging in Windows Server 2003 .....	5-9
Enabling Auditing of Hercules Software Registry Key .....	5-11
Enable Auditing of Hercules Software Registry Key in Windows 2000 .....	5-11
Enable Auditing of Hercules Software Registry Key in Windows 2003 .....	5-12
Enabling Auditing of Hercules Working Directory .....	5-16
Enable Auditing of Hercules Working Directory in Windows 2000 .....	5-16
Enable Auditing of Hercules Working Directory in Windows 2003 .....	5-17
Enabling Auditing of Hercules Databases .....	5-19
Enable Auditing of Hercules Database in Windows 2000 .....	5-19
Enable Auditing of Hercules Database in Windows 2003 .....	5-20
Enabling Auditing of Hercules Public Directory on Web Server .....	5-21
Enable Auditing of Public Directory on Web Server in Windows 2000 .....	5-21
Enable Auditing of Public Directory on Web Server in Windows 2003 .....	5-22
<b>A.Security Best Practices .....</b>	<b>A-1</b>
Security Environment .....	A-1
Controlled Environment Installation .....	A-1
Maintaining Secure Operation of Hercules in the Event of Failure .....	A-1
Configure System Failure and Recovery Options .....	A-1
Configure Audit Trail Overflow .....	A-1
V-Flash Server Secure Communication .....	A-2
Password and Access Controls .....	A-2
Password Security Requirements .....	A-2
Changing CMS User Password on Hercules Server .....	A-3
Configuring Clients for UNIX, Linux, and Mac OS X for Sudo Access .....	A-4
<b>B. Services to Shut Down .....</b>	<b>B-1</b>
Level 1 Basic Shutdown of Unnecessary Services .....	B-1
Level 2 Moderate Shutdown of Unnecessary Services .....	B-2
<b>R.References .....</b>	<b>R-1</b>
General .....	R-1

---

---

Hercules Level 1 and Level 2 Security Configuration Guide Patch List .....	R-1
National Security Agency Recommendation Guides .....	R-1
Windows 2000 Common Criteria Security Configuration Guide .....	R-1
Windows Server 2003 Security Guide .....	R-1
Security Innovations in Windows Server 2003 .....	R-1
Microsoft Internet Information Services .....	R-1
Internet Information Services 5.0 Lockdown Tool .....	R-1
Guide to Secure Configuration and Administration of Microsoft IIS 5.0 .....	R-1
CA Certificates and SSL .....	R-2
Certificates .....	R-2
Guide to Secure Configuration and Administration of Windows 2000 Certificate Services .....	R-2
How to Set Up SSL on a Web Server .....	R-2
How to Set Up Client Certificates .....	R-2
Step-by-Step Guide to Setting Up a Certification Authority .....	R-2
Microsoft Certificate Services Using Windows Server 2003 .....	R-2
System Failure .....	R-2
How to Configure System Failure and Recovery Options in Windows .....	R-2

# Before You Begin

---

## Purpose

The purpose of the *Hercules Security Configuration Guide* is to provide a checklist for securing your Hercules installation at the operating system level with corresponding step-by-step procedures.

The expectation is that you will apply one security change at a time, observe the results, and determine whether modification or backing out the setting is indicated, based on site criteria. This process is intended to begin as soon as you begin to use Hercules for vulnerability remediation and/or policy enforcement. Until you are using Hercules in this way, you will not be able to properly evaluate the impact of the security change in a production environment.

## Audience

This document is written to the Hercules administrator who is responsible for securing the server machines on which the Hercules Server, Hercules Channel Server, and Hercules Download Servers are installed.

## About this Manual

The *Hercules Security Configuration Guide* describes configuration of IIS, certificates and SSL configuration, audit logging, and security best practices. Procedures apply to both Microsoft Windows 2000 Server and Windows Server 2003.

Checklist items are ordered in the recommended implementation order.

## Documentation Map

The Hercules system includes the following documents that are available as PDF files from the Help menu in the Hercules Administrator and are also installed at the Hercules Administrator and Hercules Server install path, typically C:\Program Files:

[InstallPath]\Citadel\Hercules\Administrator\Help

- **Vulnerability Assessment and Remediation Overview** – Assists you in planning an assessment and remediation strategy using Hercules and its associated tools.
- **Hercules Quick Start Guide** – Provides overview information about the Hercules System benefits, best practices and a walkthrough procedure.
- **Hercules Installation Guide** – Provides requirements, license information, and install and uninstall procedures for the Hercules Server, Hercules Channel Server, Hercules Download Server, and the Hercules Administrator.
- **Hercules User's Guide** – Provides detailed procedures for operating the Hercules system, including managing servers, devices, clients, remedies, vulnerabilities, ActionPacks, Policies, Remediations and Policy Enforcements. The same information is also provided as context-sensitive help.

- **Hercules Remedy Actions Reference** – Describes the properties and acceptable values for each Citadel- provided remedy action.
- **Creating Network Install Package for Microsoft Internet Explorer 6.0** – Provides instructions for setting up a Microsoft Internet Explorer IEAK installation package for installing on Hercules Servers.
- **Using Hercules and Administrative Network Installation Points to Remediate Microsoft Office 2000** – Provides instructions for creating a network administrative installation package to apply Microsoft Office service packs using Hercules remediation.

Hercules also makes available a *Hercules Security Configuration Guide* which describes configuration of IIS, certificates and SSL configuration, audit logging, and security best practices. Contact Citadel for information on this document.

## Online Help

**Hercules Administrator Context-Sensitive Help** provides the same information as the Hercules User's Guide. When you click on the Help button or press F1 in any window or dialog box of the Hercules Administrator, the system displays a context-sensitive topic. Click on the links to navigate to other topics.

## Contacting Support

When you purchase a Customer Support Agreement and register your Citadel software product, you are eligible to receive technical support according to the terms of the contract you purchased. Registered users may reach Citadel Customer Support through the toll-free hot line at 888-9-CITADEL, (888-924-8233), by e-mail at [support@citadel.com](mailto:support@citadel.com), or through the Customer Support Portal on the Citadel website at <http://www.citadel.com/>.

Business hours for telephone support are Monday through Friday, excluding holidays, from 8 a.m. until 6 p.m., U.S. Central Standard Time. When you call, please have the following information available:

- Hercules version number
- Hercules serial number
- Type of hardware

---

# 1. Hercules® Security Recommendations

---

## Introduction

The *Hercules Security Configuration Guide* provides procedures for securing the Hercules® Server, Hercules Channel Server and Hercules Download Server v3.5, after the initial installation and configuration of the product. This document defines how to configure the Hercules system to comply with Common Criteria Evaluation Assurance Level 3 (EAL3) requirements established in the Hercules Security Target. The procedures apply both to Microsoft® Windows® 2000 Server and Windows Server™ 2003; differences are noted where applicable. This document provides security configuration recommendations for Hercules using two levels of security.

## Assumptions

This document assumes that the Hercules Server, Hercules Channel Server, and Hercules Download Server have been installed on dedicated Windows 2000 Server or Windows Server 2003 machines that provide no other services on your network and that the Hercules Administrator has been installed on a machine which may or may not be used for other user-space tasks. The following assumptions are used in this guide:

- Before you upgraded the Hercules Server from versions 2.2.1 or 3.0.1 to version 3.5, you created a verified backup of the current installed Hercules server. For backup instructions, see the *Hercules Users's Guide*.
- The server or servers on which you installed the Hercules Server, Hercules Channel Server, and Hercules Download Server meet the following requirements:
  - Have an installed image of the Windows 2000 Server or Windows Server 2003 families.
  - Have at least the minimum hardware defined in the *Hercules Installation Guide*.
  - Have default loads of the required services (no additional services were added).
  - Have no third party applications running.
  - Have no Microsoft applications (such as Microsoft Internet Security and Acceleration Server, etc.) running except Microsoft Internet Information Services, Microsoft .NET v1.1 Framework, and for Windows Server 2003, ASP.NET.

## Securing Hercules

Resources on the Internet that provide guides and checklists for securing a Windows 2000 Server installation include Microsoft, SANS™ (SysAdmin, Audit, Network, Security) and the NSA/CSS (National Security Agency/Central Security Service). This document focuses on securing your Hercules installation using the "[Windows 2000 Common Criteria Security Configuration Guide](#)" on page R-1 and the "[National Security Agency Recommendation Guides](#)" on page R-1. Appendix E of the *Windows 2000 Common Criteria Security Configuration Guide* provides a checklist of settings recommended to increase the basic operating system security of your Hercules installation.

## **Hercules Architecture**

The Hercules system is designed with a distributed web-based architecture and is available in a stand-alone or distributed configurations. See the *Hercules User's Guide* Chapter 1: "Hercules System Overview" for descriptions and diagrams of each and a description of each server component.

## Configuration Recommendations for Hercules Server

Information specific to configuring Windows Server 2003 security is provided in the ["Windows Server 2003 Security Guide" on page R-1](#). Additional information on Windows Server 2003 security can be found at ["Security Innovations in Windows Server 2003" on page R-1](#).

### Hercules Security Levels

Citadel™ provides security configuration recommendations that allow you to secure the Hercules Server at two levels.

- Level 1 recommendations provide *basic security* configurations for the different types of Hercules servers.
- The Level 2 security recommendation is equivalent to a *moderate level lockdown* for the servers.

**WARNING:** The security configurations for the Hercules Servers, Hercules Channel Server, and Hercules Download Servers should not be applied to other devices on your network.

In addition, Hercules also recommends applying certain patches and hot fixes. You should use these security recommendations in accordance with your own network security policies.

Hercules maintains a website with the latest security remedy changes: ["Hercules Level 1 and Level 2 Security Configuration Guide Patch List" on page R-1](#).

### Update Patches and Hot Fixes on all Types of Hercules Servers

The Patches remedy group will update all patches and hot fixes that are currently provided by Microsoft. For a current list of updates and patches, see ["Hercules Level 1 and Level 2 Security Configuration Guide Patch List" on page R-1](#). Citadel will update the security patch remedies via the V-Flash server as Microsoft releases additional hot fixes and updates.

### Level 1 - Baseline Security Configuration

#### Internet Information Services Lockdown

These are basic Internet Information Services (IIS) lockdown recommendations to secure your Microsoft Web Server. This is a manual step that is not automated with a Hercules remedy group. For details, see ["Secure Microsoft Internet Information Services 5.0 for Hercules" on page 2-1](#). Microsoft IIS 6.0 is already locked down.

#### Basic Shutdown of Unnecessary Services

These are the Level 1 basic service configuration recommendations that are completed by the Level 1 Configuration remedy group in the Hercules database. For a current list of unnecessary services that are shut down by the Level 1 remedy group, see ["Level 1 Basic Shutdown of Unnecessary Services" on page B-1](#).

### **Securing Hercules Channel Server and Download Server Web Pages**

Securing the Active Server Pages (ASPs) of the Hercules Channel Server and the Hercules Download Server is a manual step. For details, see “Preventing Anonymous Access to Hercules Channel Server ASPs” and “Preventing Anonymous Access to Hercules Download Server ASPs” in the *Hercules Installation Guide* section on Post Installation Setup. These procedures prevent anonymous access to the Hercules Channel Server and Hercules Download Server ASPs. Once set, any unauthorized user without authentication is prevented from accessing the Hercules Channel Server through a web browser and modifying entries in the ASP pages. Implementing these procedures is a requirement; not a recommendation.

### **Allowing Sudo Access for Hercules Servers and Devices**

Allowing sudo access for Hercules servers and devices is a manual step. For details, see the *Hercules User's Guide* section, “Configure Clients for UNIX, Linux, and Mac OS X for Sudo Access.” Sudo allows pre-defined users to have temporary root access to run CMS commands (install/uninstall, start/stop, reboot, and remediate). This increases the level of trust in the user performing CMS operations. Using sudo is optional, but recommended for Level 1.

### **Basic Microsoft SQL Server 2000 Desktop Engine Configurations**

Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) is the free, redistributable version of SQL Server that serves as the Hercules embedded database. The lockdown step for MSDE 2000 is a manual step--not automated with a Hercules remedy group. For details, see "[MSDE Level 1 Security Recommendation](#)" on page 1-9. These are basic SQL security configurations for the Microsoft SQL Server Data Engine (MSDE) only. If you use these security configurations on the Microsoft SQL Server, you should consult first with your database administrator. If Microsoft SQL Server is installed on the same machine as the Hercules servers, you should contact Technical Support, since its use may be restricted to applications running only on that server.

### **Basic Microsoft SQL Server 2000 Configurations**

#### **Basic Auditing**

These auditing recommendations are for IIS audit logging only and are partially automated with the Level 1 Configuration remedy group. For details on the manual configuration steps, see "[Auditing All Types of Hercules Servers](#)" on page 5-7.

## **Level 2 - Moderate Security Configuration**

The Level 2 basic service configuration recommendations include everything in the Level 1 Configuration remedy group, plus anything else that is not necessary for Hercules functionality.

### **Moderate Shutdown of Unnecessary Services**

This part of the lockdown process is completed by the Level 2 Configuration remedy group in the Hercules database. For a current list of services that are shut down by the Level 2 remedy group, see “Level 2 Moderate Shutdown of Unnecessary Services” on page B-2.

## Directory and User Security

These are security configurations for restricting access to Hercules directories and disabling access to unnecessary users. This is a manual step in the lockdown process and is not automated with a Hercules remedy group. For details, see the following:

- ["Restricting User and Group Access to Any Type of Hercules Server" on page 3-1.](#)
- ["Restricting Access to Hercules Working Directories" on page 3-4](#)
- ["Restricting Access to Hercules Databases" on page 3-10](#)

## Configuring SSL

As a part of Level 2 security configurations, Citadel recommends that SSL be used with the Hercules Server, Hercules Channel Server and Hercules Download Servers. This is a manual process that is not automated by using the Level 2 security remedy group. For details, see ["Using SSL and Certificates" on page 4-1.](#)

## Moderate Microsoft SQL Server 2000 Desktop Engine Configurations

These are moderate SQL security configurations for the MSDE 2000 only. If you would like to use these security configurations on the Microsoft SQL Enterprise server, you should consult first with your database administrator. This is a manual step in the lockdown process and is not automated with a Hercules remedy group. For details, see ["Level 2 Moderate Shutdown of Unnecessary Services" on page B-2.](#)

## Moderate Auditing

These auditing recommendations are for auditing the Hercules software registry key, working directory, database, and the public directory on the web server. The recommendations are partially automated with the Level 2 Configuration remedy group. The procedures apply to the Hercules Server, Hercules Channel Server, and Hercules Download Server. For details on the manual configuration steps, see the following:

- ["Enabling Auditing of Hercules Software Registry Key" on page 5-11](#)
- ["Enabling Auditing of Hercules Working Directory" on page 5-16](#)
- ["Enabling Auditing of Hercules Databases" on page 5-19](#)
- ["Enabling Auditing of Hercules Public Directory on Web Server" on page 5-21](#)

## Role-Based Authorization

Hercules provides role-based authorization capability to allow only approved system administrators to perform certain procedures. For example, role-based authorization allows only approved system administrators, device group administrators, or remedy writers to create and modify custom remedies. This feature adds additional security layered infrastructure to Hercules. You can assign Trustees to pre-defined Roles. In the Hercules Administrator you can associate Roles with Trustees. Trustees are individual users; user groups are not supported by Hercules. For details, see page 1-22 of the *Hercules User's Guide* for "Role-Based Security" under "Hercules Security Mechanism."

## Enforce the Security Patches and Level 1 or Level 2 Configuration Policies

Citadel-supplied policies include the following three security policies:

- Citadel - Hercules 3.5—Baseline Security Template - Patches
- Citadel - Hercules 3.5—Level 1 Baseline Security Template - Configurations
- Citadel - Hercules 3.5—Level 2 Baseline Security Template - Configurations

For *Baseline security*, enforce the following two policies in this sequence:

1. Citadel - Hercules 3.5—Baseline Security Template - Patches
2. Citadel - Hercules 3.5—Level 1 Baseline Security Template - Configurations

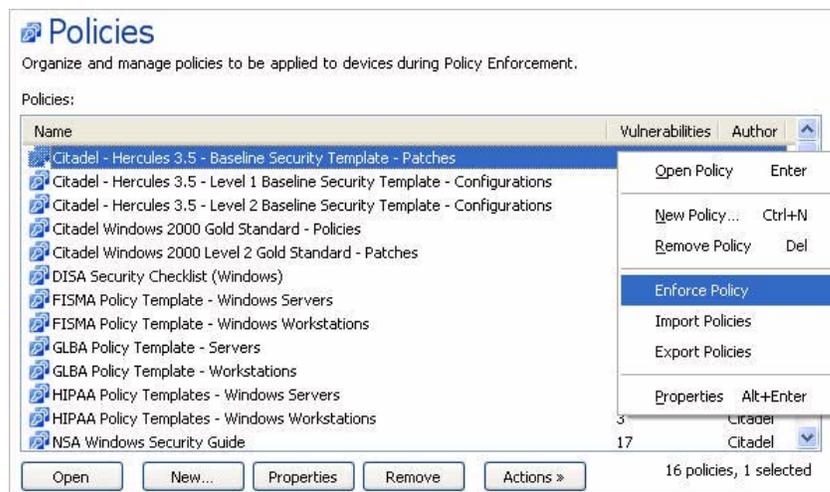
For *moderate security*, enforce the following two policies in this sequence:

1. Citadel - Hercules 3.5—Baseline Security Template - Patches
2. Citadel - Hercules 3.5—Level 2 Baseline Security Template - Configurations

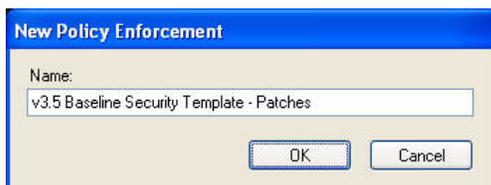
The Level 2 Configurations policy includes all of the configuration remedies for Level 1, as well as those for Level 2 security. The remedies for all Configuration policies will return either Success or Failure but never Compliant.

Follow these steps to create a Policy Enforcement that will apply the policy for Baseline Security Template - Patches to the device or devices on which the Hercules Server, Hercules Channel Server, and Hercules Download Server are installed. Use the same procedure to enforce the Level 1 or Level 2 Baseline Security Template - Configurations except select the Level 1 or Level 2 Baseline Security Template.

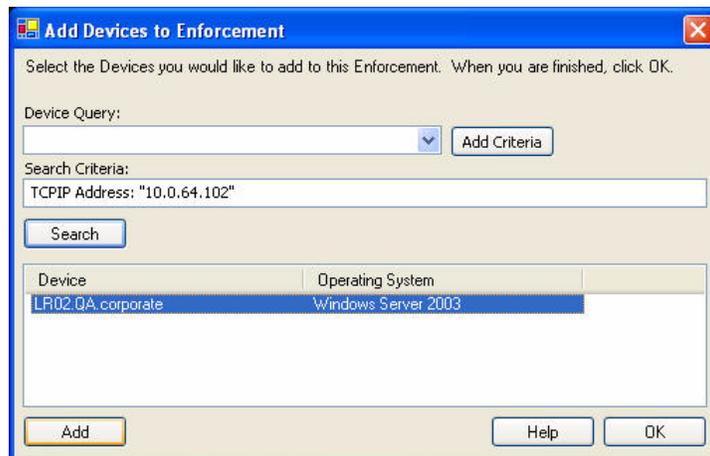
1. In the Navigation pane, click **Policies** to open the Policies page.



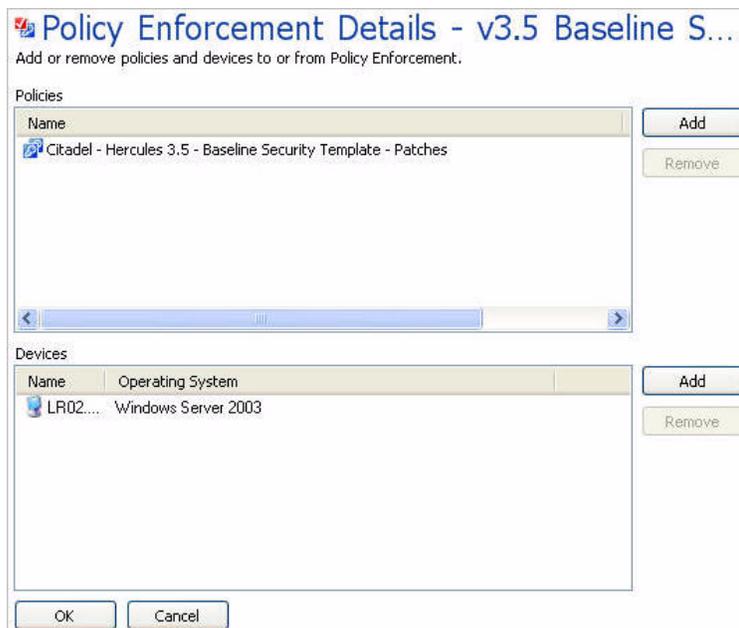
2. In the **Policies** list, right-click **Citadel - Hercules 3.5—Baseline Security Template - Patches** and then click **Enforce Policy** to open New Policy Enforcement.



3. Type in a name for the Policy Enforcement and click **OK** to open Policy Enforcement Details.
4. Click the **Add** button next to the Devices pane to open Add Devices to Enforcement.



5. Click **Add Criteria** to open Available Search Attributes. Select an attribute from the list. If all Hercules servers are installed on the same machine, select TCP/IP Address and click **Add**. Enter the IP address between the pair of quotation marks and click **Search**. Verify that the displayed device is correct, then select it and click **Add**. Then, click **OK** to display Policy Enforcement Details.



**WARNING:** You should apply this particular policy *only* to the server or servers on which a Hercules Server, the Hercules Channel Server, and a Hercules Download Servers are installed.

6. To save the changes and exit, click **OK** to open a confirmation to save. Click **OK** to open Scheduled Tasks.

### Scheduled Tasks

Manage schedules of all configured policy enforcements and remediations.

Scheduled Tasks:

Task Name	Next Occurrence	Task Type
v3.5 Baseline Security Template - Patches	Not scheduled	Policy Enforcement

1 scheduled tasks, 1 select

7. Click **Properties** to open Policy Enforcement Properties. Accept or change the start event interval, then click **OK** to open Scheduled Tasks.

### Scheduled Tasks

Manage schedules of all configured policy enforcements and remediations.

Scheduled Tasks:

Task Name	Next Occurrence	Task Type
v3.5 Baseline Security Template - Patches	Starts: 10/29/2004 5:29:57 PM within: 1 Hour	Policy Enforcement

Review	Enter
View Progress	
Delete	Del
Properties	Alt+Enter

8. Select **View Progress** to open the Remediation Progress tab in the Welcome to the Hercules Operations Center. Monitor to view the successful policy enforcement. The new Policy Enforcement is displayed in the list.

## Securing the Microsoft Data Engine (MSDE)

### Hercules Databases

Hercules installs the Microsoft SQL Server 2000 Desktop Engine (MSDE 2000) version of Microsoft SQL Server, unless Microsoft SQL Server is already installed on the machine. This section lists several recommendations for securing the MSDE only. If you would like to use these security configurations on Microsoft SQL server, you should consult first with your database administrator.

### MSDE Level 1 Security Recommendation

The following security configurations are recommended for Level 1:

- The MSDE should be updated with the latest service packs and hot fix patches in order to protect against known security vulnerabilities. Existing deployments of MSDE 2000 will be running with Service Pack 3a, while all new installations will use MSDE 2000A.
- The default SA password should be changed. The new password should be no less than eight characters and comprised of a mixture of upper and lower case letters and numbers.

*Note:* Because the SA password will be duplicated at each Hercules site, Citadel recommends changing the SA password after installation.

- User accounts should be restricted on three levels:
  - Accounts should only be granted access to the databases that are required.
  - Accounts should only have access to the database objects (tables, procedures, functions) needed.
  - Accounts should only be granted permission to access or manipulate data based on their type of role (select / insert / update / delete).

### MSDE Level 2 Security Recommendation

The following security configurations are recommended for Level 2:

- Authentication should be set to use Windows Authentication and disable mixed mode. Only users or applications that have valid Windows NT® logins should be able to access the MSDE database.
- The MSDE service account should be restricted to only the necessary privileges.



---

## 2. Securing Microsoft® IIS for Hercules®

---

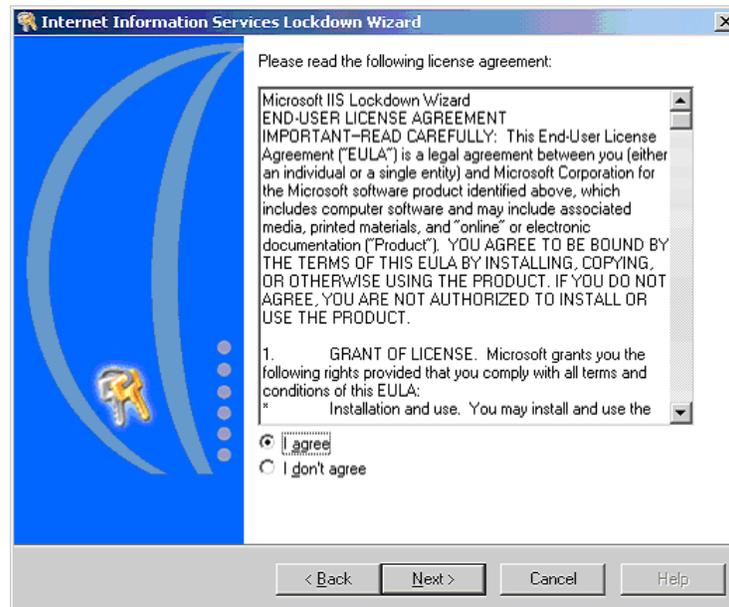
### Secure Microsoft Internet Information Services 5.0 for Hercules

Windows 2000 OS includes the built-in Web server, Internet Information Services 5.0. Once the basic operating system has been secured you should further harden your IIS 5.0. You should have applied all outstanding software patches and hot fixes during the operating system steps. Follow this procedure to configure IIS 5.0 on any Windows 2000 Server machines where the Hercules Server, Hercules Channel Server and/or File Download Servers are installed.

1. Verify that your IIS installation is fully patched.
2. "[Internet Information Services 5.0 Lockdown Tool](#)" on page R-1. The IIS Lockdown Wizard starts. Click **Next** to display the License Agreement page.

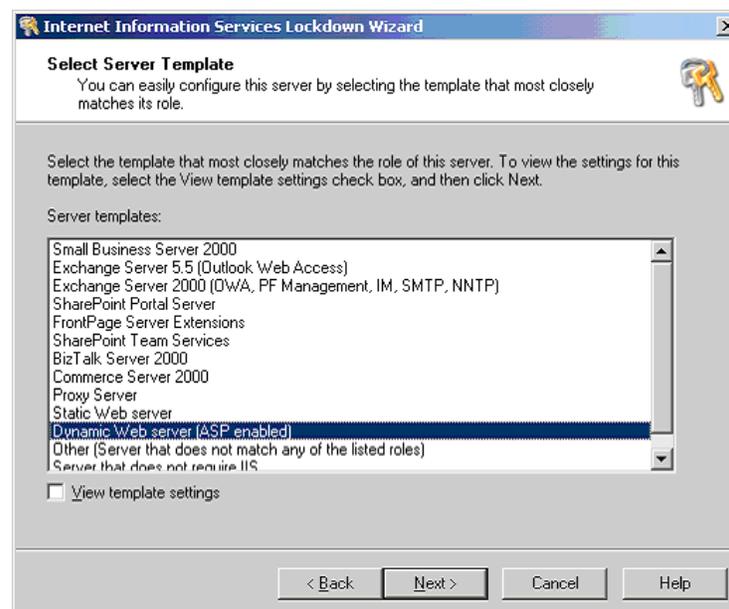


3. To accept the license agreement, select **I agree** and click **Next**.



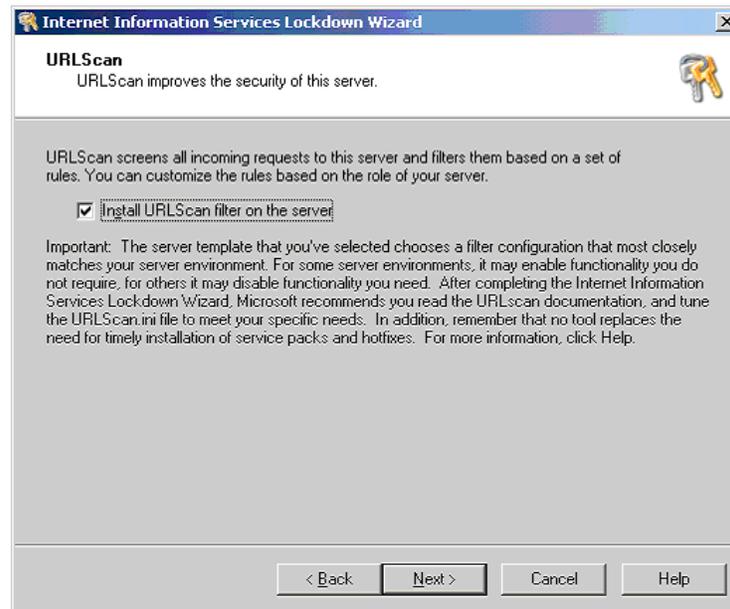
4. Select **Dynamic Web Server (ASP enabled)** as the base template for your Hercules Server, Hercules Channel Server or File Download Server. Click **Next** to continue.

*Note:* Citadel recommends you make this selection. The rest of the instructions in this procedure are based on this assumption.



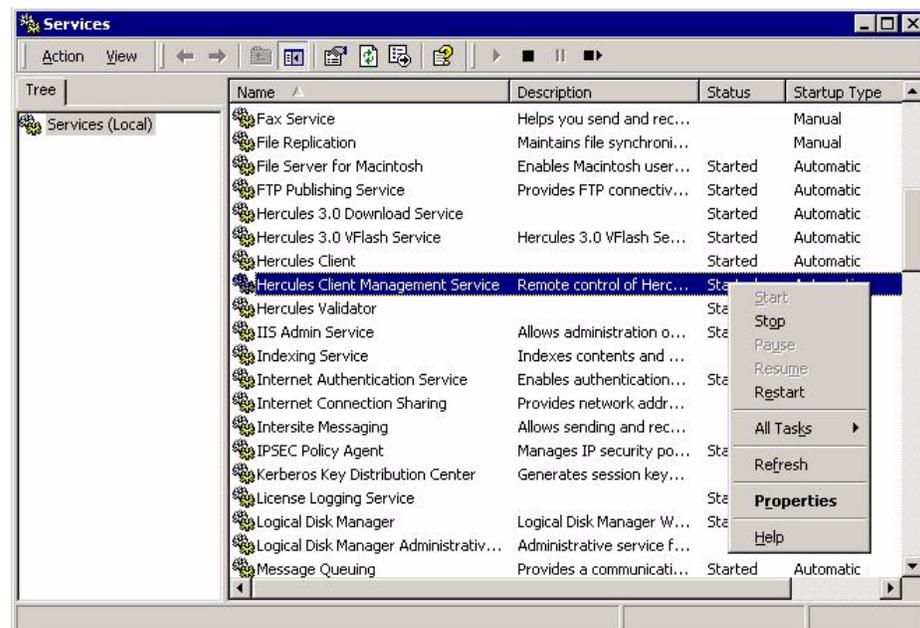
5. To filter incoming requests to your Hercules Server, Hercules Channel Server, or File Download Server, Citadel recommends you select **Install URLScan filter on**

the server. Click Next.



The final page, Ready to Apply Settings, displays the configuration you selected to apply to your Hercules Server, Hercules Channel Server, or File Download Server.

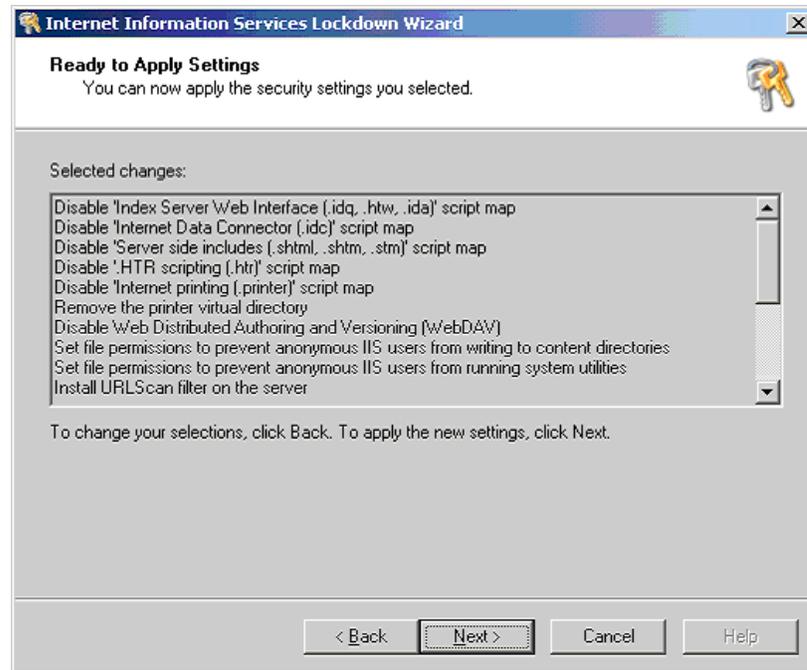
6. Before proceeding, you will need to stop some services. From the desktop, select Start > Programs > Administrative Tools > Services.
7. In the **Services** window right-hand pane, scroll to locate **Hercules Client Management Service** and right-click on it. Select **Stop**.



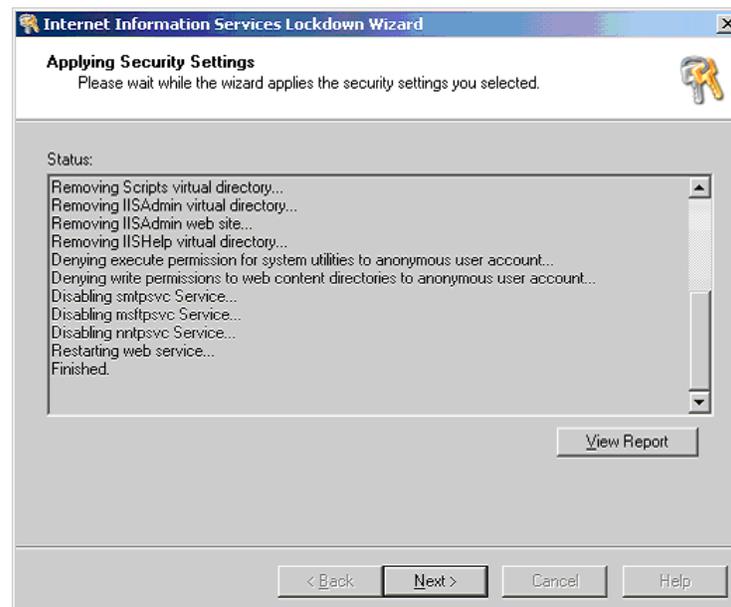
8. Repeat step 7 to stop **Hercules 3.0 Download Service** and **Hercules 3.0 Vflash Service**.

**Note:** If you do not manually stop these services, the IIS Lockdown will fail to apply your configuration.

9. Once these services are stopped, click **Next** to apply the settings.



10. Wait while IIS Lockdown applies your configuration and installs URLScan. When completed, click **Next**.



11. To exit the wizard, click **Finish**.



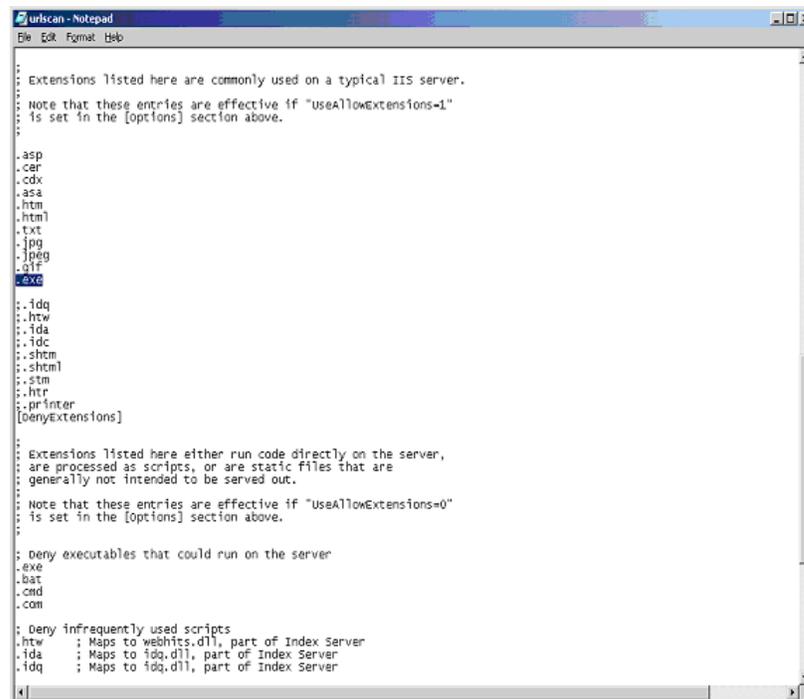
12. After completing the installation of URLScan, you will need to modify its configuration for proper Hercules Server, Hercules Channel Server, or File Download Server functionality. The URLScan configuration file, `urlscan.ini`, is located by default in

```
<SystemRoot>\System32\inetsrv\urlscan
```

where <SystemRoot> is your root directory path, for example

```
C:\WINNT\System32\inetsrv\urlscan
```

13. Open the `urlscan.ini` file and find the section labeled **[AllowExtensions]**. Add `.exe` to the list of allowed extensions, as shown below.



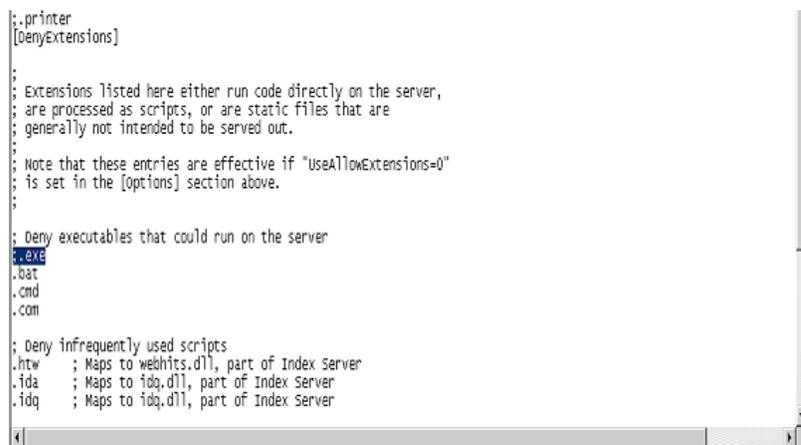
```

urlscan - Notepad
File Edit Format Help

:
: Extensions listed here are commonly used on a typical IIS server.
: Note that these entries are effective if "UseAllowExtensions=1"
: is set in the [options] section above.
:
:
: .asp
: .cer
: .cdx
: .asa
: .htm
: .html
: .txt
: .jpg
: .jpeg
: .gif
: .exe
:
: .idq
: .htw
: .ida
: .idc
: .shhtm
: .shhtml
: .stm
: .htr
: .printer
[DenyExtensions]
:
: Extensions listed here either run code directly on the server,
: are processed as scripts, or are static files that are
: generally not intended to be served out.
: Note that these entries are effective if "UseAllowExtensions=0"
: is set in the [options] section above.
:
: Deny executables that could run on the server
: .exe
: .bat
: .cmd
: .com
:
: Deny infrequently used scripts
: .htw ; Maps to webhits.dll, part of Index Server
: .ida ; Maps to idq.dll, part of Index Server
: .idq ; Maps to idq.dll, part of Index Server

```

14. In the `urlscan.ini` file, locate the section labeled **[DenyExtensions]** and remove `.exe` from the list. You can do this either by deleting the entry or by adding a semicolon in front of the entry (shown below) to comment it out.



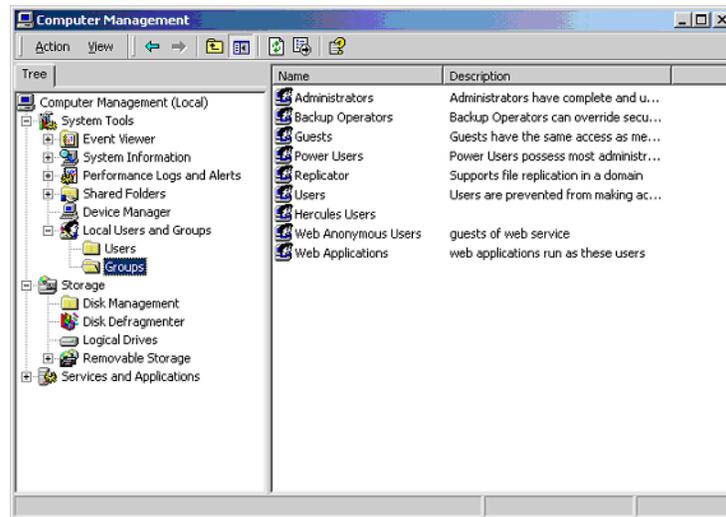
```

: .printer
[DenyExtensions]
:
: Extensions listed here either run code directly on the server,
: are processed as scripts, or are static files that are
: generally not intended to be served out.
: Note that these entries are effective if "UseAllowExtensions=0"
: is set in the [options] section above.
:
: Deny executables that could run on the server
: ;.exe
: .bat
: .cmd
: .com
:
: Deny infrequently used scripts
: .htw ; Maps to webhits.dll, part of Index Server
: .ida ; Maps to idq.dll, part of Index Server
: .idq ; Maps to idq.dll, part of Index Server

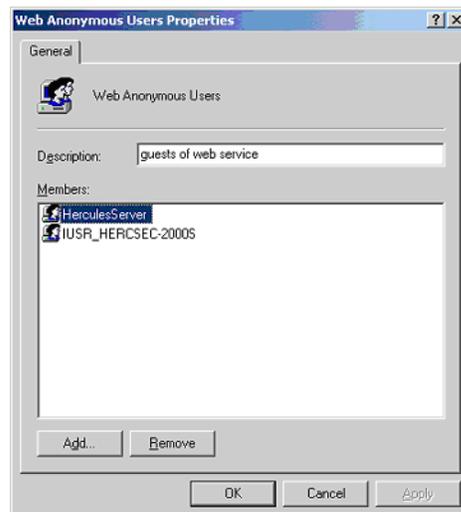
```

15. You must also modify the group membership of the HerculesServer local user on your Hercules Server, Hercules Channel Server, or File Download Server. To do this, select Start > Programs > Administrative Tools > Computer Management.

16. Expand the **Local Users and Groups** node and select the **Groups** folder.



17. In the right-hand pane, double-click **Web Anonymous Users** group.  
 18. In the members pane at the bottom, select **HerculesServer** and click **Remove**.



19. From the desktop, select **Start > Programs > Administrative Tools > Component Services**.  
 20. In the Component Services window navigation pane, click **Services**.  
 21. Right-click on **World Wide Web Publishing Service** and click **Stop**. Then right-click on it again and click **Start**.  
 22. Start the **Hercules 3.0 VFlash Service**, **Hercules Client Management Service**, and **Hercules 3.0 Download Service**.



## 3. Securing Hercules® Folders & Files

### Securing Directories and Files for Hercules Server

These procedures describe how to configure Access Control List (ACL) settings to restrict access to the Hercules Server, the Hercules Channel Server, or the File Download Server from the Hercules Administrator. During the installation of the servers, the system creates the *Hercules Users* group. Hercules grants this group full rights to access the Hercules Server, Hercules Channel Server, or the File Download Server from the Hercules Administrator, without granting the group full administrative control of the machine on which it is running.

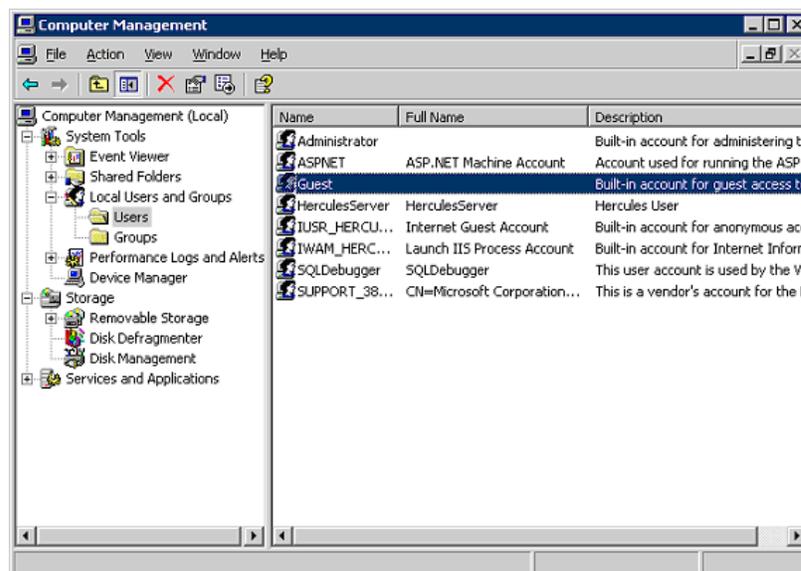
To limit access to the Hercules Server, Hercules Channel Server or File Download Server, you must restrict access to certain Hercules files and turn off anonymous access to the servers.

#### Restricting User and Group Access to Any Type of Hercules Server

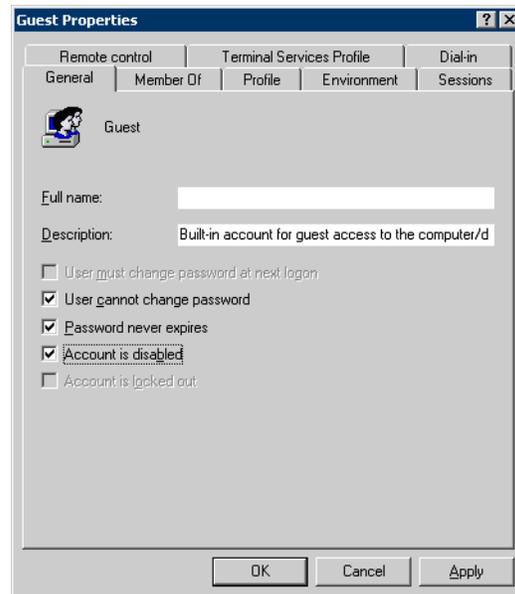
##### Restrict User and Group Access in Windows 2000

You must disable access to the Hercules Server, Hercules Channel Server and File Download Server for all unnecessary users. The following users should be the only ones that remain active: Administrator, ASPNET, HerculesServer, and IWAM\_<ServerName>. Additional users assigned to administer the Hercules Server should be added to the **Administrator** group and/or the **Hercules Users** group. The following procedure describes how to disable access to unnecessary users and groups:

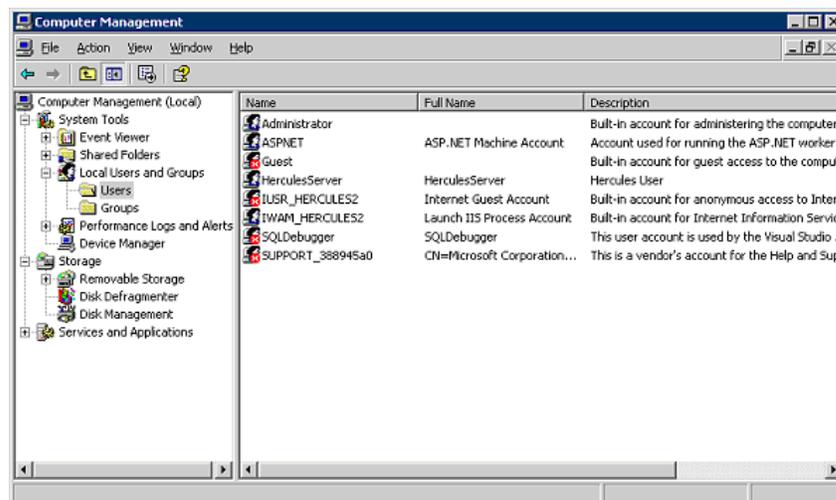
1. From the Hercules Server, Hercules Channel Server, or File Download Server desktop, select Start > Programs > Administrative Tools > Computer Management.
2. In the Computer Management window, expand **System Tools** to display **Users**.



3. To disable guests, in the right-hand pane, select **Guest** and double-click on it.
4. In the Guest Properties dialog box, select the **Account is disabled** check box and click **OK**.

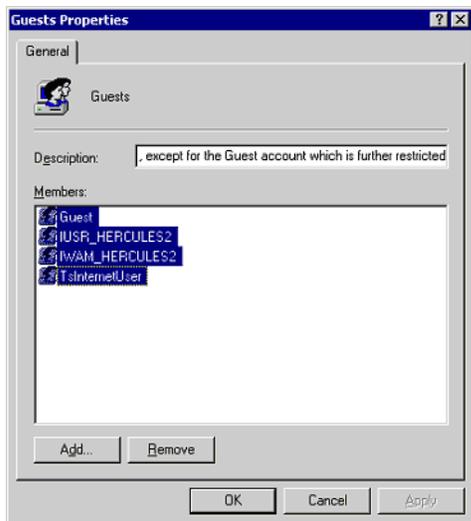


5. Repeat steps 3 and 4 for all other unnecessary users. The results are displayed in the Computer Management window, right-hand pane:



6. In the left-hand pane, select the **Groups** folder.
7. In the right-hand pane, select **Guest** and double-click on it.

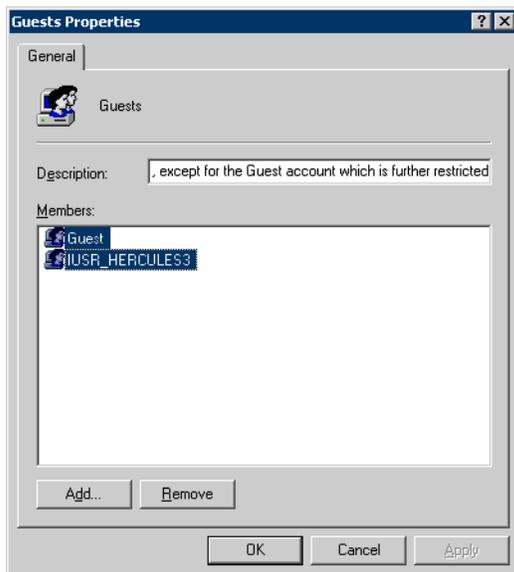
8. In the Guests Properties dialog box, in the **Members** list, select all the members listed and click **Remove**.



### Restrict User and Group Access in Windows 2003

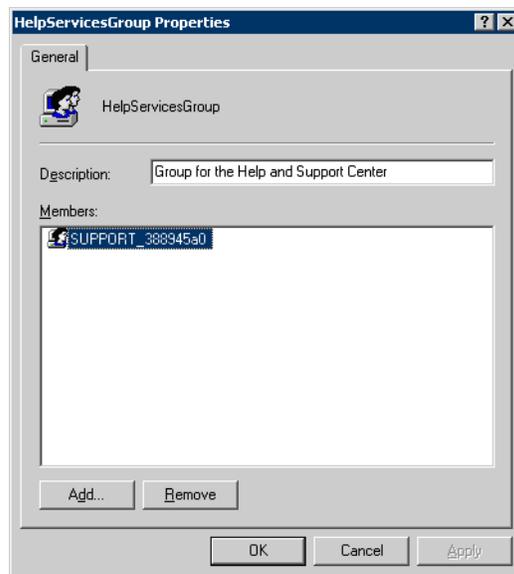
The procedures for restricting user and group access in Windows 2003 are the same as those for Windows 2000, except that you need to restrict two groups.

1. Follow steps 1-7 in ["Restrict User and Group Access in Windows 2000" on page 3-1](#).
2. In the Guests Properties dialog box, in the **Members** list, select all the members listed and click **Remove**.



3. In the Computer Management window, in the left-hand pane, select the **Groups** folder.
4. In the right-hand pane, select **HelpServicesGroup** and double-click on it.

- In the HelpServicesGroup Properties dialog box, in the **Members** list, select the **Support\_388945a0** member and click **Remove**.

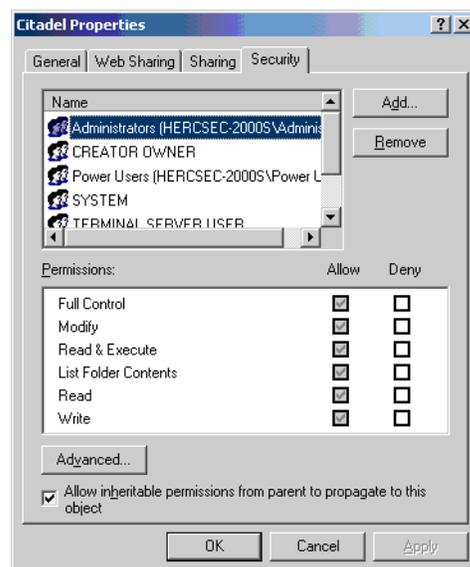


## Restricting Access to Hercules Working Directories

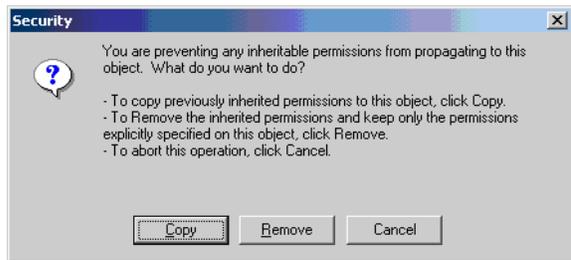
You should restrict access to the Hercules working directory in the Hercules Server, Hercules Channel Server, and File Download Server installations. By default, Hercules will install to `C:\ProgramFiles\Citadel`.

### Restrict Access to Hercules Working Directory in Windows 2000

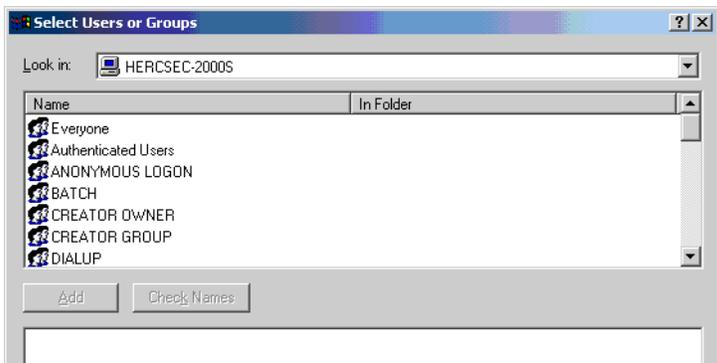
- Navigate to `<Hercules Install Path>\Citadel` and right-click on it. Select **Properties**.
- In the Citadel Properties dialog box, click on the **Security** tab.
- Clear the **Allow inheritable permissions** check box near the bottom.



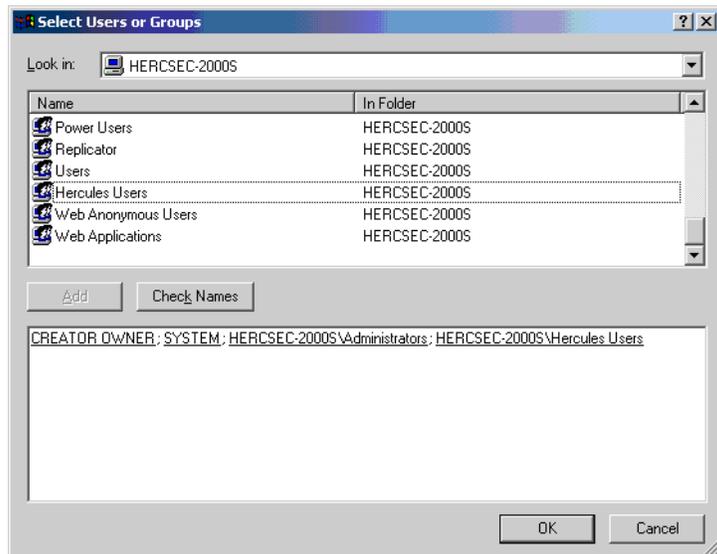
4. To remove inheritable permissions, click **Remove** at the prompt.



5. In the Citadel Properties dialog box, click the **Add** button near the top.
6. In the **Look in** drop-down list, change the location to your local system.

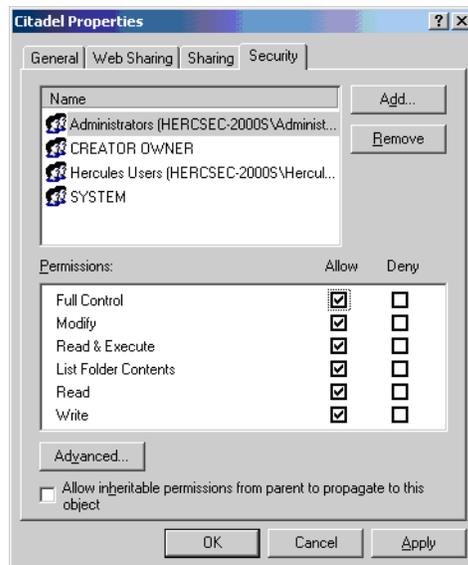


7. From the list at the top, select **CREATOR OWNER, SYSTEM, Administrators, and Hercules Users** and click **Add**.



8. To apply the changes, click **OK**.

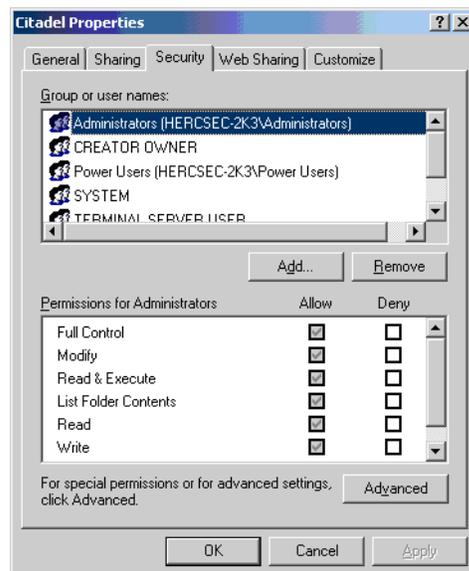
- In the Citadel Properties dialog box, from the list near the top, select **Administrators** and then select the **Full Control** check box under **Allow**.



- Repeat step 9 for each of the users you added in step 7.
- Click **OK** to apply these permissions.

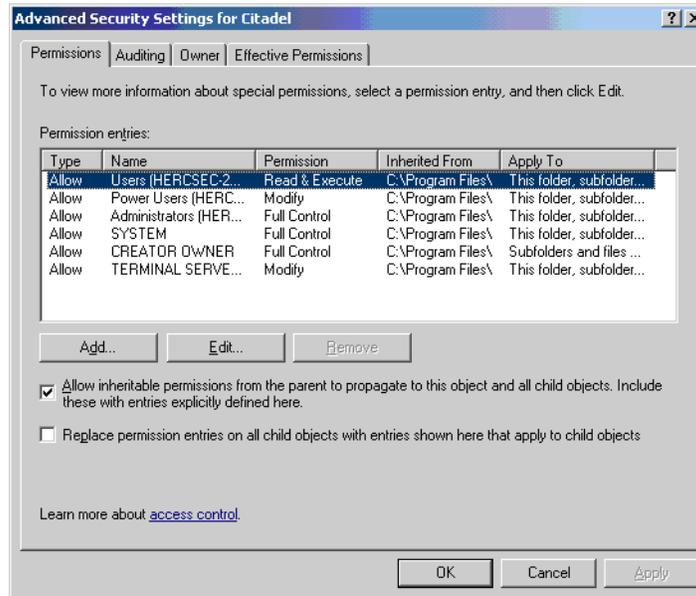
### Restrict Access to Hercules Working Directory in Windows 2003

- Navigate to <Hercules Install Path>\Citadel and right-click on it. Select **Properties**.
- In the Citadel Properties dialog box, click on the **Security** tab.

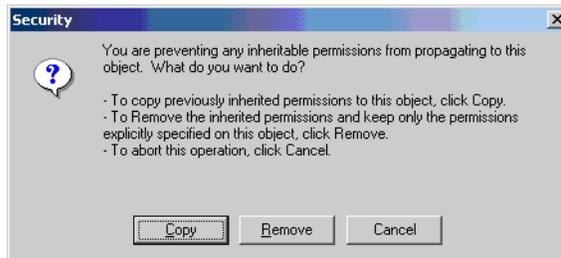


- Click on the **Advanced** button near the bottom.

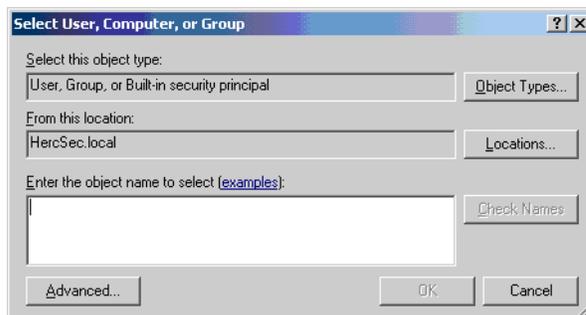
4. Clear the **Allow inheritable permissions** check box near the bottom.



5. To remove inheritable permissions, click **Remove** at the prompt.

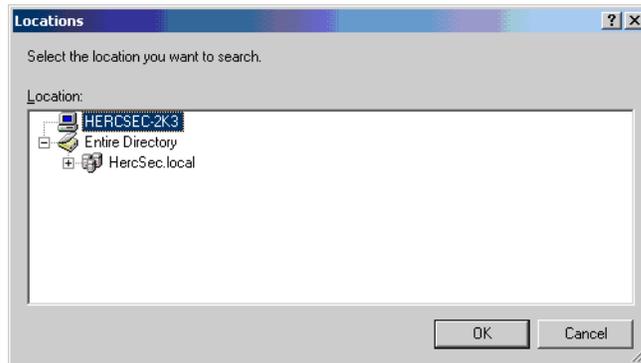


6. In the Advanced Security Settings dialog box, click the **Add** button. The Select User, Computer, or Group dialog box displays.

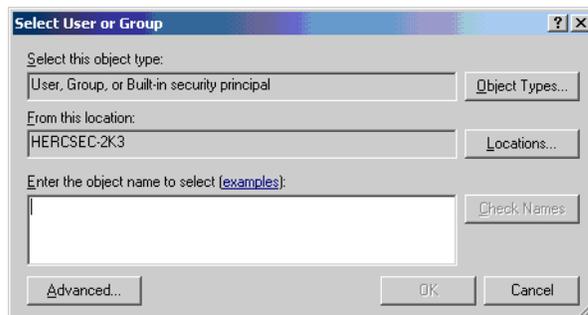


7. Click on the **Locations** button.

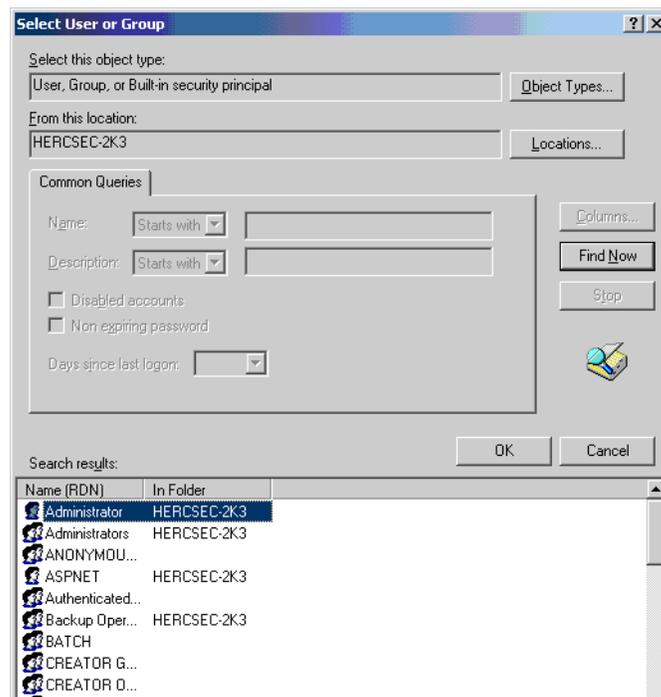
8. Select your local server and click **OK**.



9. In the Select User or Group dialog box, click **Advanced**.

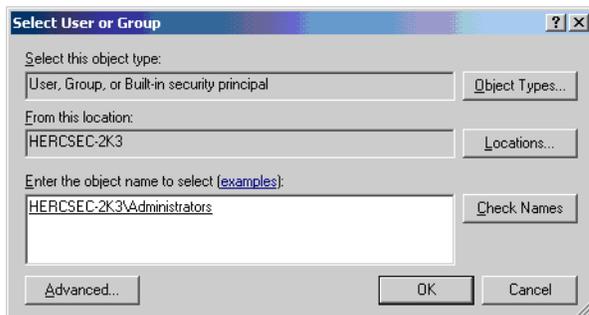


10. To search for the list of Local Users, click **Find Now**.

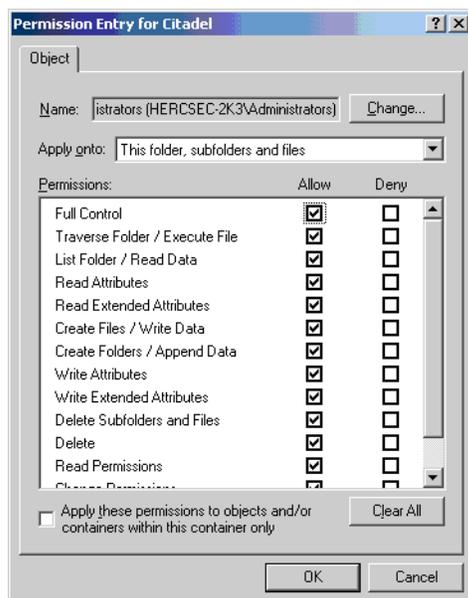


11. From the **Search results** list, select **Administrators** and click **OK**. This will add the

Administrators group to the Select User or Group dialog box.



12. Click **OK**.
13. In the Permissions Entry dialog box, click **Full Control** under **Allow**.



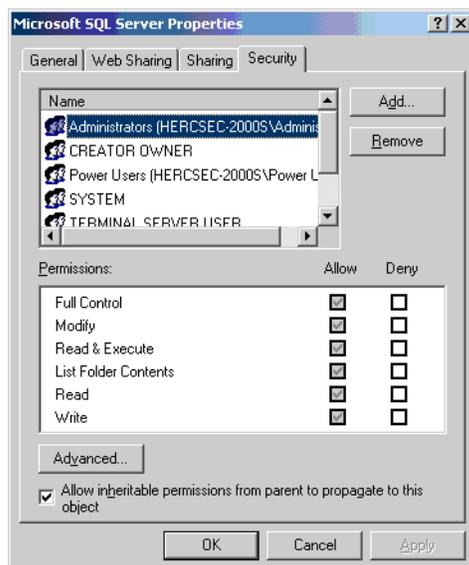
14. To apply these permissions to the Citadel directory, click **OK**.
15. Repeat steps 9 to 14 for **CREATOR OWNER**, **Hercules Users** and **SYSTEM**.
16. In the Citadel Properties dialog box, click **OK** to finish setting permissions.

## Restricting Access to Hercules Databases

The following directory security should be applied to the Hercules Server, Hercules Channel Server, and File Download Server installations. By default, Hercules will install to `C:\ProgramFiles`.

### Restrict Access to Hercules Databases in Windows 2000

1. Navigate to <Hercules Install Path>\ and right-click on the **Microsoft SQL Server** folder. Then select **Properties**.
2. In the Microsoft SQL Server Properties dialog box, click on the **Security** tab.
3. Clear the **Allow inheritable permissions** check box near the bottom.

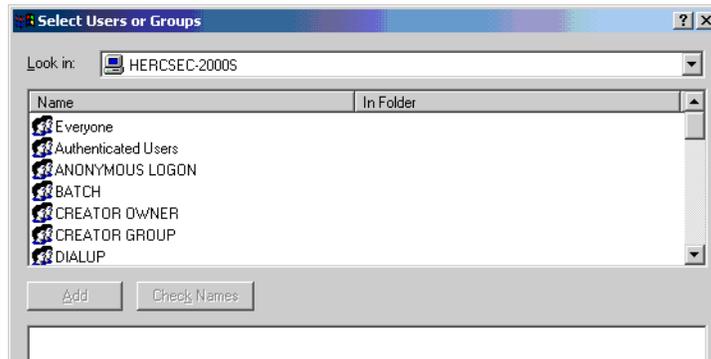


4. To remove inheritable permissions, click **Remove** at the prompt.

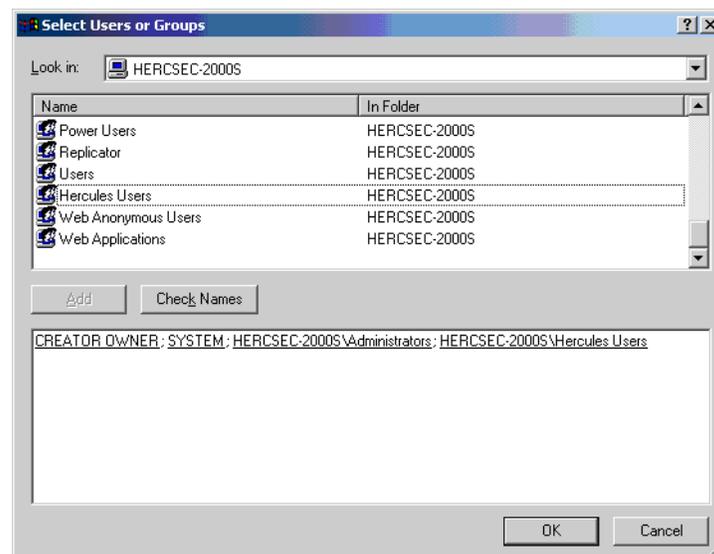


5. In the Microsoft SQL Server Properties dialog box, click the **Add** button near the top.

6. In the **Look in** drop-down list, change the location to your local system.

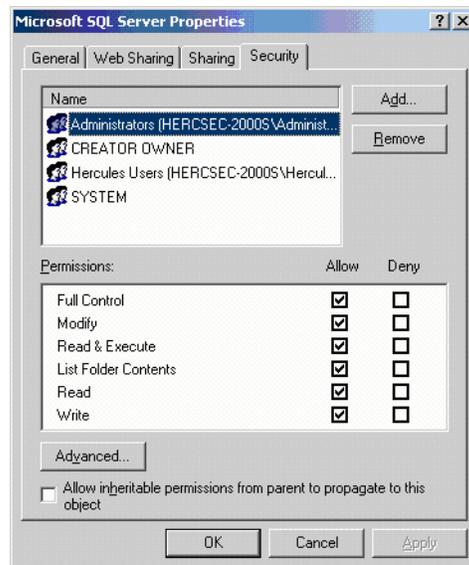


7. From the list at the top, select **CREATOR OWNER**, **SYSTEM**, **Administrators**, and **Hercules Users** and click **Add**.



8. To apply the changes, click **OK**.

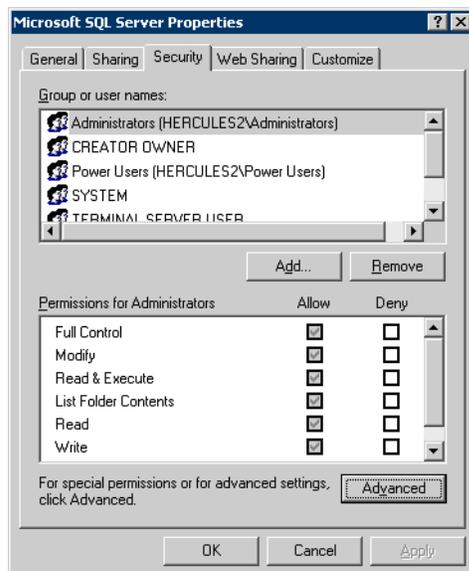
- In the Microsoft SQL Server Properties dialog box, from the list near the top, select **Administrators** and then select the **Full Control** check box under **Allow**.



- Repeat step 9 for each of the users you added in step 7.
- Click **OK** to apply these permissions.

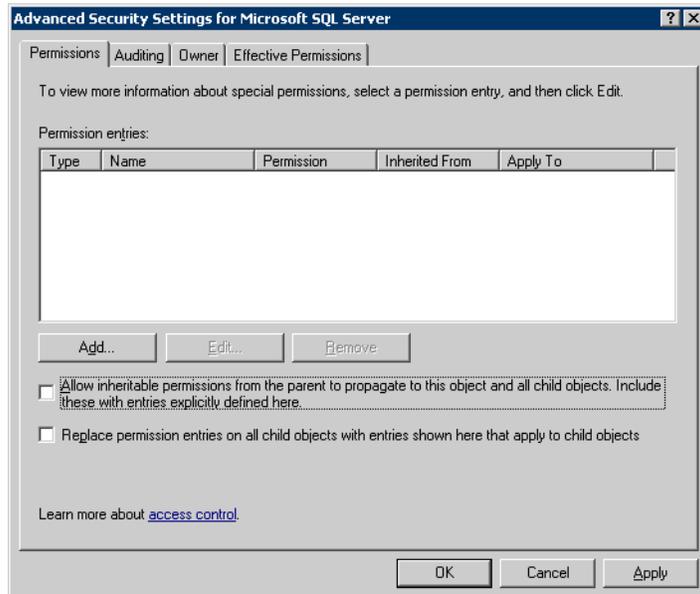
### Restrict Access to Hercules Database in Windows 2003

- Navigate to <Hercules Install Path> and right-click on the **Microsoft SQL Server** folder. Then select **Properties**.
- In the Microsoft SQL Server Properties dialog box, click on the **Security** tab.

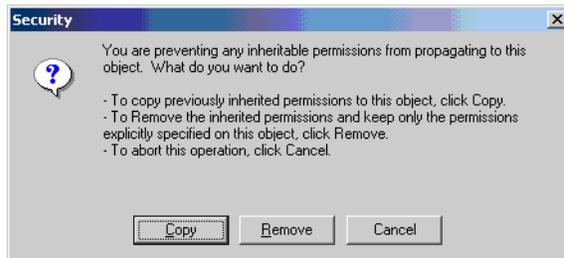


- Click on the **Advanced** button near the bottom.

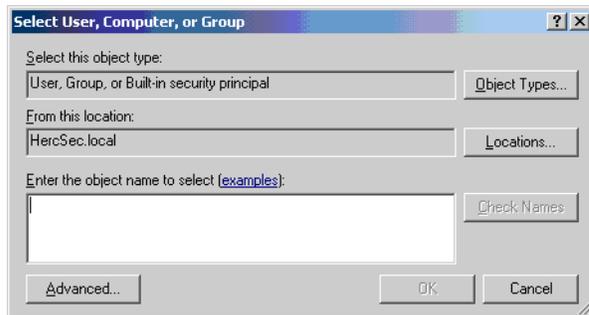
4. Clear the **Allow inheritable permissions** check box near the bottom.



5. To remove inheritable permissions, click **Remove** at the prompt.

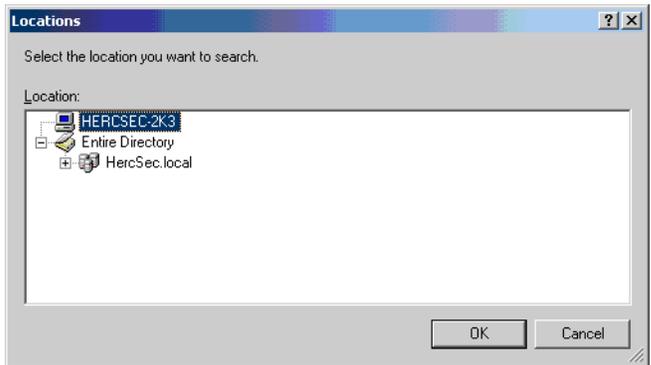


6. In the Advanced Security Settings dialog box, click the **Add** button. The Select User, Computer, or Group dialog box displays.

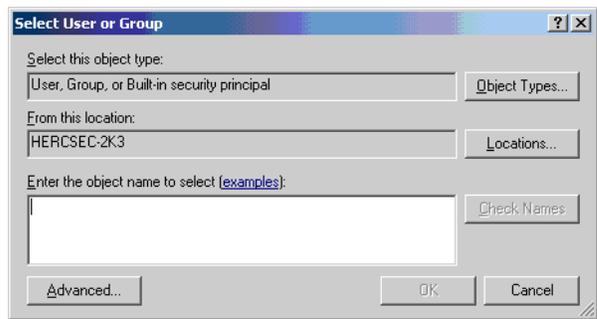


7. Click on the **Locations** button.

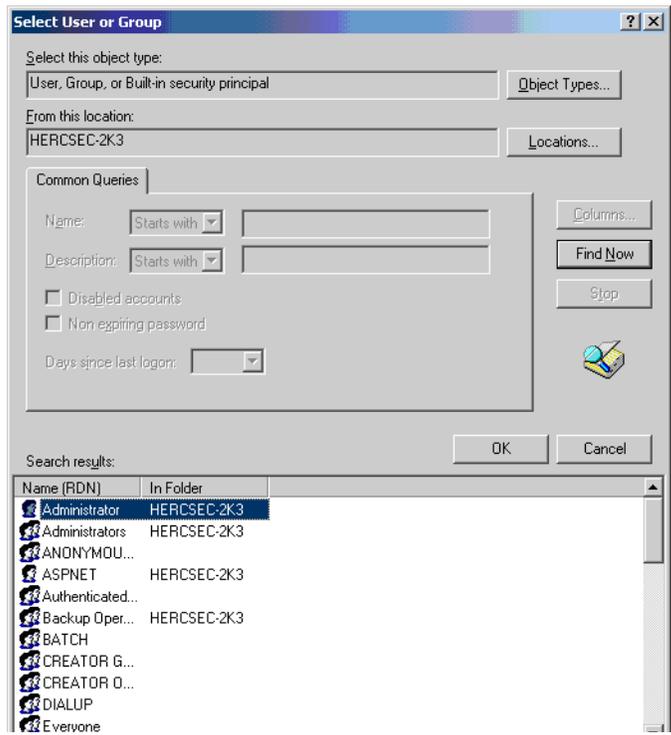
- 8. Select your local server and click **OK**.



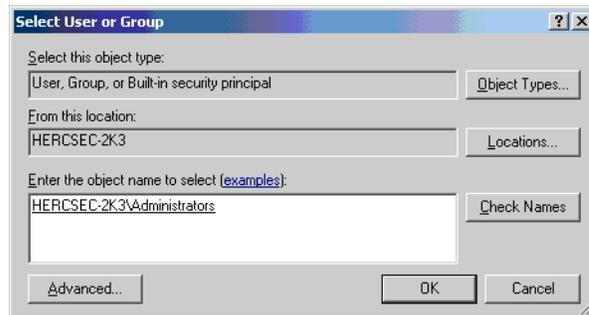
- 9. In the Select User or Group dialog box, click **Advanced**.



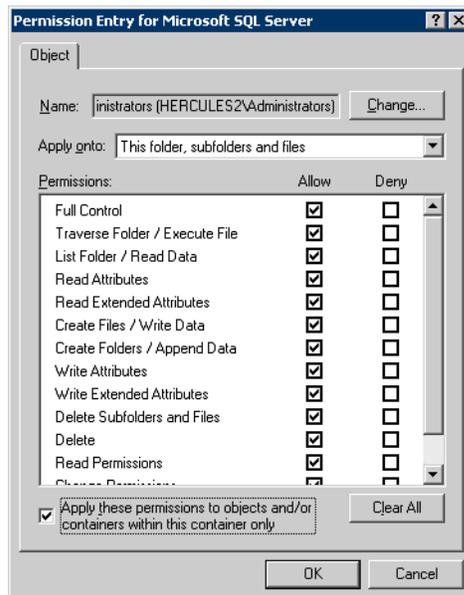
- 10. To search for the list of Local Users, click **Find Now**.



- From the **Search results** list, select **Administrators** and click **OK**. This will add the Administrators group to the Select User or Group dialog box.



- Click **OK**.
- In the Permissions Entry dialog box, click **Full Control** under **Allow**.



- To apply these permissions to the Microsoft SQL Server directory, click **OK**.
- Repeat steps 9 to 14 for **CREATOR OWNER**, **Hercules Users** and **SYSTEM**.
- In the Citadel Properties dialog box, click **OK** to finish setting permissions.



---

## 4. Configuring SSL in Hercules® System

---

### Using SSL and Certificates in the Hercules System

This section describes how to use SSL and certificates, public and private keys, and the different types of certificates and certificate authorities. It also includes information on how to prepare to configure SSL in Hercules Servers.

#### Using SSL and Certificates

Secure Socket Layer (SSL) is the standard security protocol for secure communications over the Internet. SSL allows for a secure *pipe* to be established between two entities. SSL uses digital certificates in transactions to validate that both parties are who they say they are. In Level 2, Hercules addresses best practices for security and uses SSL to provide strong authentication, as well as encryption.

#### Public and Private Key Certificates and Certificate Authority

A public-key certificate (PKC) is a digital certificate that attests that an entity, such as the Hercules Client, is bound to a public key value. The certification comes from a third party, called a Certificate Authority (CA). A certificate contains the name and public key component of the user and vouches to the truth and accuracy of the information it contains.

To use certificates successfully, you must have a general understanding of how certificates work. Following are some useful references:

- ["Certificates" on page R-2](#), from Microsoft TechNet
- ["Guide to Secure Configuration and Administration of Microsoft IIS 5.0" on page R-1](#)

#### Certificate Types

Depending on the type of authentication, Hercules requires three types of certificates, CA root certificates, CA server certificates, and CA client certificates. The CA server certificate contains a public key for the Hercules Server or the Hercules Download Server and the CA client certificate contains a public key for the Hercules Client. The CA certificate, also known as a CA root certificate, contains a private key that represents the last step in a validation chain and indicates that the public and private keys are valid. Every time a Client connects with the Hercules Server or the Hercules Download Server, their public keys are validated with the CA root certificate, before a connection can be established.

#### Hercules Server and Hercules Download Server Certificates

For one-way and two-way authentication, the Hercules Server needs a CA root certificate and a unique CA server certificate. For communicating across the network, the Hercules Download Server also needs a CA root certificate and a unique CA certificate. For additional information, see ["How to Set Up SSL on a Web Server" on page R-2](#).

## Hercules Client Certificates

For one-way and two-way authentication, the Hercules Client needs a CA root certificate. For two-way authentication, the Hercules Client also needs a unique CA client certificate. For additional information, see ["How to Set Up Client Certificates" on page R-2](#).

## Certificate Authority

There are many ways to obtain certificates for Hercules, but the easiest way is to purchase a certificate from a third-party CA. You can also create your own CA (see ["Step-by-Step Guide to Setting Up a Certification Authority" on page R-2](#)). For additional information on how to set up a certificate authority using Microsoft Certificate Services, see ["Microsoft Certificate Services Using Windows Server 2003" on page R-2](#).

## Preparing to Configure SSL in Hercules Servers

The Hercules system can operate in a standalone localhost mode where communication among the three Hercules servers reside within the same machine or in a distributed environment where all Hercules components communicate across the network. This section describes how to enable SSL and HTTP for Hercules Clients for UNIX, Linux, and Mac OS X, how to perform additional encryption configuration of clients for Windows NT, and how to uninstall Hercules Clients for Microsoft Windows.

### Enable SSL and HTTPS for Clients for UNIX, Linux and Mac OS X

Before Hercules Clients for UNIX and Linux can be configured for secure communications, SSL and HTTPS need to be enabled using OpenSSL. The minimum requirements are OpenSSL 0.9.6 and OpenSSH 3.5p1, for all clients except the Mac OS X, which requires OpenSSH 3.6p1.

*Note:* To enable SSL and SSH on Solaris 8, install patch 112438-01.

Verify that OpenSSL is installed by issuing the following commands:

1. To verify that OpenSSL has been installed and to get the version of OpenSSH, issue  

```
ssh -v
```
2. To verify the version of OpenSSL that is installed, issue this command:  

```
openssl version
```

### Configure 128-bit Encryption in Hercules Clients

All Hercules Clients must be configured for 128-bit encryption. This requires additional configuration for clients for Windows NT 4.0 Server and Windows NT 4.0 Workstation. To use 128-bit SSL communication on Windows NT, you must first install one of these:

- 128-bit encryption Service Pack
- Microsoft Internet Explorer 6.0 with Service Pack 1

### Uninstall Hercules Clients for Microsoft Windows

If you are configuring SSL on an existing Hercules installation, Citadel recommends that you uninstall all Hercules Clients for Microsoft Windows before configuring SSL and reinstall them after configuring SSL. See "[Reinstall Hercules Clients for Microsoft Windows \(1-Way\)](#)" on page 4-12. Follow these steps to uninstall a client using CMS (for details, see the *Hercules User's Guide*):

**Note:** You should not uninstall Hercules Clients for UNIX, Linux, and Mac OS X.

1. Launch the Hercules Administrator and select the desired Hercules Server.
2. Open the Manage Device Groups window, right-click on the desired device group, and then click **Uninstall Hercules Client from Devices**.
3. In the Navigation pane, under **Operations**, click **Monitor device actions**.
4. Monitor the status of the devices until each of their status changes from **Queued** to **Succeeded**.
5. If a client fails to uninstall, verify that it is connected by clicking on the **Device Communications** tab and keep retrying to uninstall.

All Hercules clients must be uninstalled successfully before proceeding.

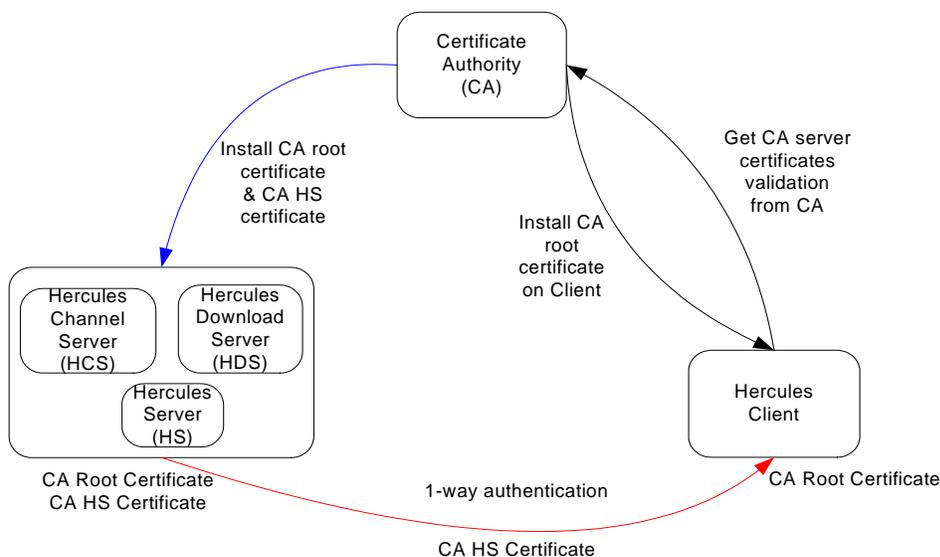
6. Repeat steps 1 to 5 for all device groups in the server.

## Configuring SSL in Hercules System Using Localhost Mode

This section describes how to configure SSL in the Hercules system to use one-way and two-way authentication while operating in localhost mode, where communications between the Hercules Server (HS), the Hercules Download Server (FDS) and the Hercules Channel Server (HCS) reside within the same machine.

### Configuring Hercules to Use Certificates With 1-Way Authentication

The following graphic illustrates the process for 1-way authentication. The Hercules Server requests a CA server certificate and the CA root certificate, while the Hercules Client independently requests the CA root certificate. The Hercules Client uses the CA root certificate to authenticate the Hercules Server's CA server certificate, which allows the Hercules Client to authenticate the Hercules Server's communication. The Hercules Administrator supports the same secure communications as the Hercules Client.



### Overview of Setting Up SSL and Certificates in Hercules (1-Way)

This section describes the following procedures for setting up SSL communication capability on Hercules and enabling SSL communications between the Hercules Server and the Hercules Administrator and Clients:

1. ["Requesting and Installing CA Certificates on the Hercules Server \(1-Way\)"](#) on page 4-5
2. ["Uninstall Hercules Clients for Microsoft Windows"](#) on page 4-3
3. ["Configure Hercules Clients for UNIX to use CA Root Certificate \(1-Way\)"](#) on page 4-5
4. ["Configure the Hercules Administrator to use SSL \(1-Way only\)"](#) on page 4-6
5. ["Configure Server URLs to Use HTTPS \(1-Way\)"](#) on page 4-6
6. ["Configure HTTPS Communications to Work with CMS \(1-Way only\)"](#) on page 4-8
7. ["Modify Hercules Server URL from HTTP to HTTPS in hclient.conf"](#) on page 4-10
8. ["Configure IIS to Require SSL Access \(1-Way\)"](#) on page 4-11

9. ["Reinstall Hercules Clients for Microsoft Windows \(1-Way\)" on page 4-12](#)
10. ["Restart Hercules Clients for UNIX, Linux, and Mac OS X" on page 4-13](#)

### **Requesting and Installing CA Certificates on the Hercules Server (1-Way)**

This section describes the procedures for retrieving, a CA root certificate and requesting and installing the CA server certificate:

*Note:* You will not be able to use the IP address of the machine to connect via SSL unless you have created a certificate for an IP address, rather than a host name.

1. Retrieve the CA root certificate.
2. Request a CA server certificate from your CA. For details, see ["Hercules Server and Hercules Download Server Certificates" on page 4-1](#).
3. Issue the CA server certificate.
4. Install the CA server certificate on the Web server. For details, see ["Hercules Server and Hercules Download Server Certificates" on page 4-1](#).

### **Retrieve and Install the CA Root Certificate for Clients for Windows**

This procedure is not required if you already have a CA root certificate. The Hercules Client and the Hercules Administrator need SSL plus the CA root certificate in one-way authentication. These steps provide some assistance to install the CA root certificate in either the Hercules Administrator or the Client for Microsoft Windows:

1. Retrieve the CA root certificate.
2. To install the CA root certificate, from the desktop, browse to locate the certificate file and double-click on it to open the Certificate window.
3. Click **Install Certificate** to start the Certificate Import wizard. In the Welcome page, click **Next**.
4. Select **Place all certificates in the following store** and click **Browse**.
5. Select **Show physical stores**.
6. Select **Local Computer** under the Trusted Root Certificate Store.
7. Click **OK** and then click **Next**.
8. The wizard displays the settings. Click **Finish** to exit the wizard.

### **Configure Hercules Clients for UNIX to use CA Root Certificate (1-Way)**

Follow these steps to configure Hercules Clients for UNIX and Linux to use certificates in one-way authentication:

1. ["Enable SSL and HTTPS for Clients for UNIX, Linux and Mac OS X" on page 4-2](#).
2. Download the CA root certificate to the Hercules Client.
3. Browse to the directory where you downloaded the CA root certificate.
4. To trust the CA that signed the CA server certificate, issue this command:

```
openssl x509 -hash -noout -in <CACertFile>
```

where <CACertFile> is the name of the certificate file you downloaded in step 2.

5. Now issue this command, using the hash generated in step 4:
 

```
ln -s <ca cert file> <hash>.0
```
6. Add the following entries to `\opt\citadel\Hercules\hclient.conf`:
 

```
ca_directory=<path where root CA certificates are located>
```

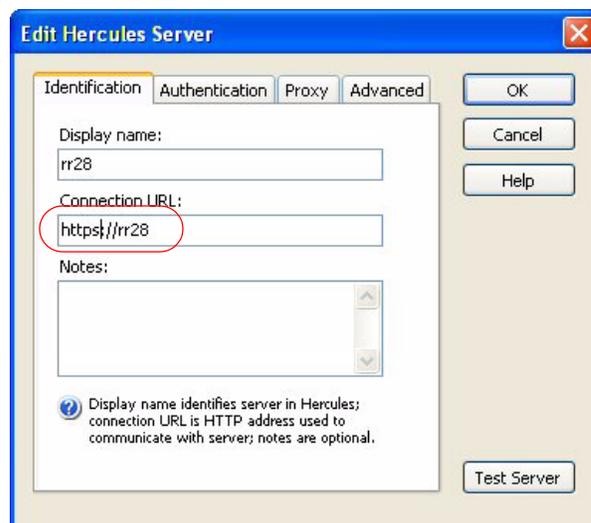
### Configure the Hercules Administrator to use SSL (1-Way only)

The Hercules Administrator needs SSL plus the CA root certificate.

1. If you do not have a CA root certificate already installed, ["Retrieve and Install the CA Root Certificate for Clients for Windows"](#) on page 4-5.
2. From the Hercules Administrator, in the navigation pane click **Servers**.
3. In the **Hercules servers** list, right-click on the desired server and click **Edit**.
4. In the Identification tab, change the **Connection URL** to

```
https://<CommonName>
```

where `<CommonName>` must match the Common Name on the server SSL certificate



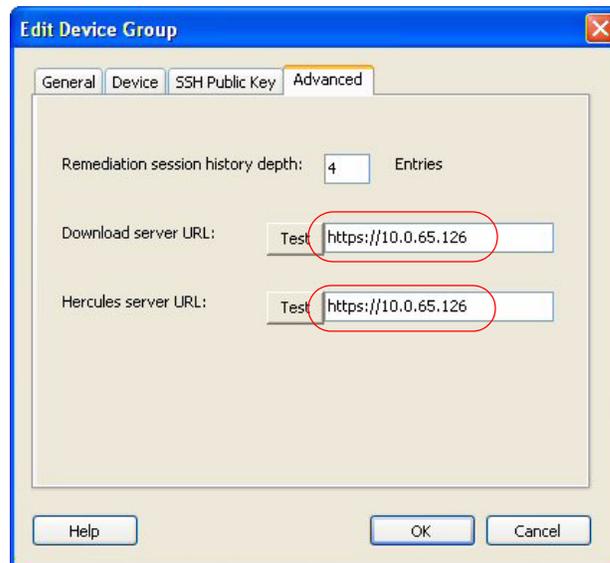
5. To verify your connection to the Hercules Server, click the **Test Server** button.
6. Click **OK** to save the changes.

### Configure Server URLs to Use HTTPS (1-Way)

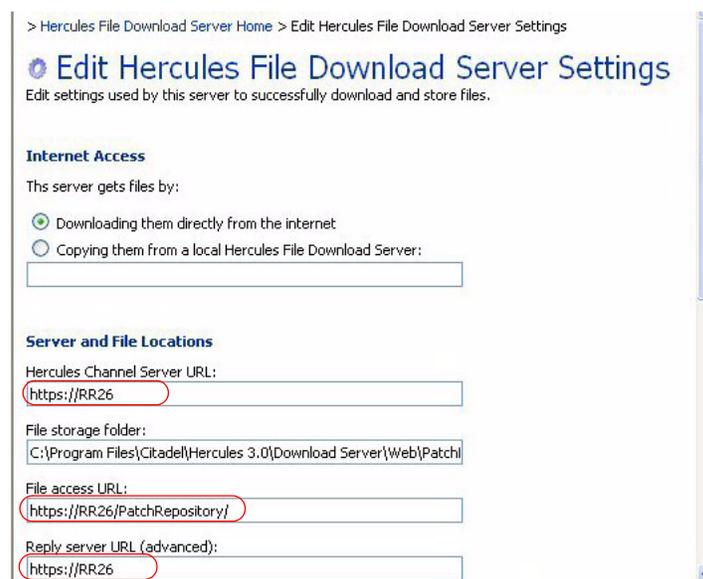
Reconfigure various server URLs used by the Hercules system by changing HTTP to HTTPS. The following procedure can be used either if you are installing the Hercules system for the first time or configuring SSL and certificates on an existing installation:

1. Launch the Hercules Administrator and select a Hercules Server.
2. In the Navigation pane, click **Manage device groups**,
3. in the Manage Device Groups window, right-click the desired device group and click **Edit Device Group**.
4. In the Edit Device Groups dialog box, click the **Advanced** tab.

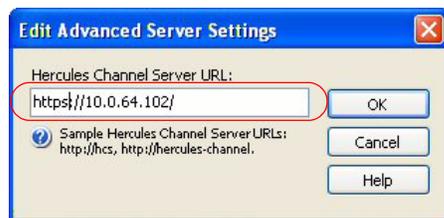
- Change the **Hercules Server URL** and the Hercules Download Server URL stored by Hercules Clients from HTTP to HTTPS.



- Verify that the Hercules Server URL and the Hercules Download Server URL match the Common Name on the certificate for each server.
- From the **Tools** menu, click **Connect to Hercules Channel Server**.
- In the Connect to Server dialog box, select **Hercules Hercules Download Server** and type **Server URL** using HTTPS.
- In the Manage and Configure Hercules Hercules Download Server web page, click **Edit Hercules Hercules Download Server Settings**.
- In the Edit Hercules Hercules Download Server Settings web page, change the HTTP settings to HTTPS for the **Hercules Channel Server URL**, **File access URL** and **Reply server URL**.



11. Verify that the Hercules Channel Server URL matches the Common Name on the certificate for each server.
12. In the Navigation pane, click **Servers**.
13. Right-click on the desired Hercules Server on the list and then click **Edit Server**.
14. In the Edit Hercules Server dialog box, click the **Advanced** tab and then click the **Advanced** button.
15. In the Edit Advanced Server Settings dialog box, change **Hercules Channel Server URL** from HTTP to HTTPS.



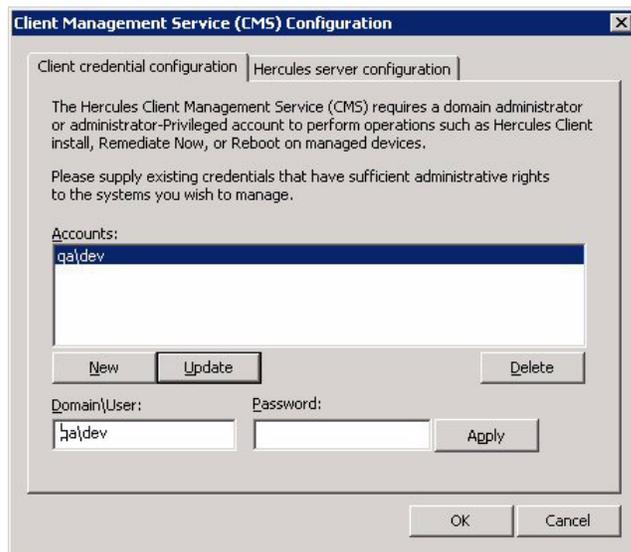
16. Verify that the Hercules Channel Server URL matches the Common Name on the certificate for each server.

### Configure HTTPS Communications to Work with CMS (1-Way only)

The Hercules Server configuration must also be modified to use HTTPS; follow these steps:

1. From the Hercules Server desktop, select Start > Run and type in  
`cmd`
2. At the DOS prompt, change to the Hercules install directory:  
`<Install Directory>\Citadel\Hercules\Services`
3. To configure the Hercules Server URL for HTTPS, type in  
`ClientMgrService -install`
4. When the Hercules Server Configuration dialog box displays, click New to enable

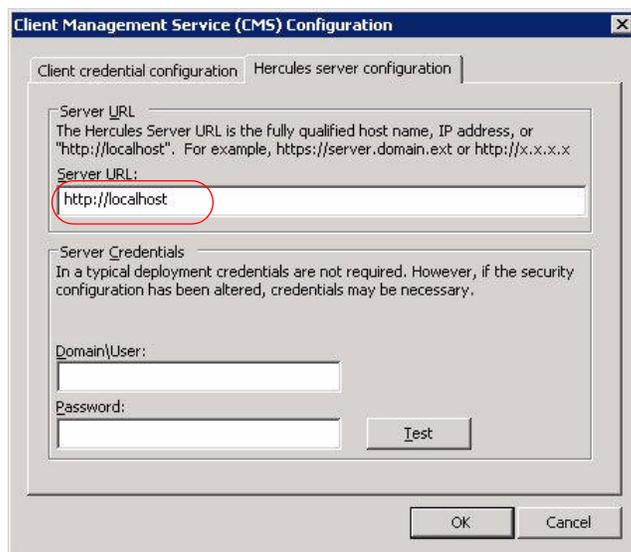
the credentials textboxes..



5. In **User Name**, type in <domain>\<user name>. Then type in the user's password and click **OK**.

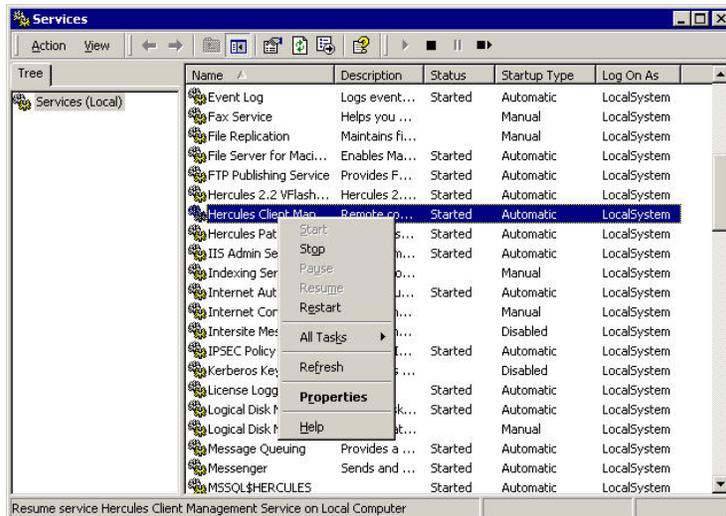
*Note:* The user name must be valid on the Hercules Server machine.

6. Tab to Hercules server configuration.



7. For **Server URL**, change HTTP to HTTPS, then click **OK**.
8. To restart CMS, select Start > Programs > Administrative Tools > Services.

9. In the **Services** window right-hand pane, scroll to locate **Hercules Client Management Service** and right-click on it. Select **Restart**.



### Modify Hercules Server URL from HTTP to HTTPS in hclient.conf

The Hercules Client for UNIX, Linux, and Mac OS X obtains its remediation information from the Hercules Server as specified in the `hclient.conf` file. You must change the URL of the server attribute in this file from HTTP to HTTPS. For details on the client configuration file, see the *Hercules User's Guide*.

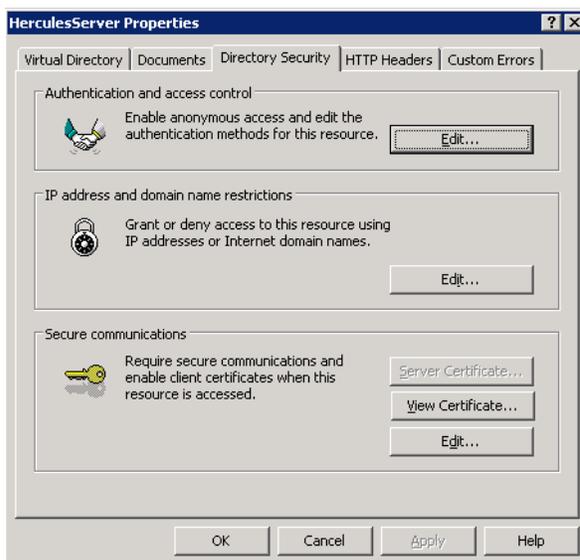
1. In the Hercules Client machine, open the Hercules configuration file located at  
`/opt/citadel/hercules/hclient.conf`
2. Modify the server property  
from `server = http://<servername>`  
to `server = https://<servername>`
3. Save the changes.

### Configure IIS to Require SSL Access (1-Way)

This procedure uses Internet Services Manager to configure a virtual directory to require SSL for access. You can require the use of SSL for specific files, directories, or virtual directories. Hercules Clients must use the HTTPS protocol to access any such resource.

**WARNING:** Once you configure for SSL access, no HTTP access will be allowed.

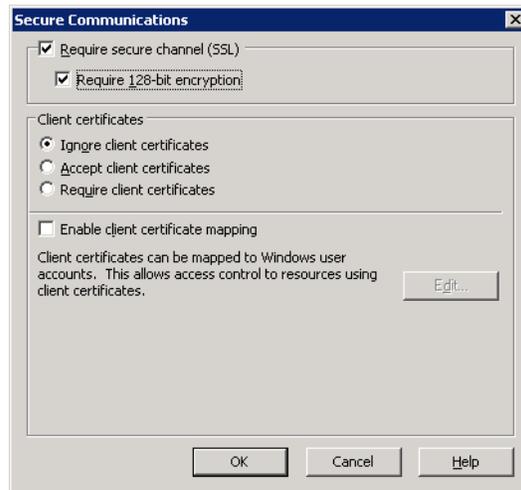
1. On the Hercules Server desktop, select Start > Administrative Tools > Internet Services Manager.
2. In the Internet Information Services (IIS) Manager window, expand your server name and then expand the **Web Sites** folder to display **Default Web Site**.
3. In the right-hand pane, locate **HerculesServer**. Right-click on it and then click **Properties**.
4. Click the **Directory Security** tab.



5. Under **Secure communications**, click **Edit**.
6. If you have Hercules Clients for Windows NT 4.0 Workstation or Windows NT 4.0 Server in your network, you must first "[Configure 128-bit Encryption in Hercules Clients](#)" on page 4-2.

7. Select the **Require secure channel (SSL)** and the **Require 128-bit encryption** check boxes. Verify that **Ignore client certificates** is selected.

*Note:* Clients browsing to this virtual directory from now on will have to use HTTPS.



8. Click **OK**, and then click **OK** again to close the **Properties** dialog box.
9. Repeat steps 3-8 for **HerculesClientService**, **PatchRepository**, **PatchService** and **HerculesChannel**.
10. Close the Internet Services Manager window. SSL is now enabled in communications between the Hercules Server and the Administrator console and the Clients.

### Reinstall Hercules Clients for Microsoft Windows (1-Way)

If you are configuring SSL on an existing Hercules installation, Citadel recommends that you uninstall all Hercules Clients for Microsoft Windows (see "[Uninstall Hercules Clients for Microsoft Windows](#)" on page 4-3) before configuring SSL and reinstall them after configuring SSL. Follow these steps to install a client using CMS:

*Note:* You do not need to reinstall Hercules Clients for UNIX, Linux, and Mac OS X (see "[Restart Hercules Clients for UNIX, Linux, and Mac OS X](#)" on page 4-13).

1. Launch the Hercules Administrator and select the desired Hercules Server.
2. Open the Manage Device Groups window, right-click on the desired device group, and then click **Install Hercules Client on Devices**.
3. In the Navigation pane, under **Operations**, click **Monitor device actions**.
4. Monitor the status of the devices until each of their status changes from **Queued** to **Succeeded**.
5. Repeat steps 1 to 4 for all groups in the server.

## Restart Hercules Clients for UNIX, Linux, and Mac OS X

After configuring SSL on an existing Hercules installation, Citadel recommends that you stop and then start the Hercules Clients for UNIX, Linux and Mac OS X. The table below describes the different start and stop commands needed for each platform

Platform	Stop Command	Start Command
Solaris™	/etc/init.d/hercules stop	/etc/init.d/hercules start
Red Hat®	/etc/rc.d/init.d/hercules stop	/etc/rc.d/init.d/hercules start
AIX®	/etc/hercules stop	/etc/hercules start
HP-UX®	/sbin/init.d/hercules stop	/sbin/init.d/hercules start
Mac OS X® <sup>a</sup>	/Library/StartupItems/Hercules/ Hercules stop	/Library/StartupItems/Hercules/ Hercules start

- a. You can use sudo instead of logging in as root; instead of stop/start, you can execute:  
/Library/StartupItems/Hercules/Hercules restart

Follow these steps to restart the Hercules clients for UNIX, Linux and Mac OS X:

**Note:** You do not need to uninstall and reinstall these clients.

1. On the client machine, from the command line, log in as root.

**Note:** On the Mac OS X, you can use sudo instead.

2. Issue the stop command appropriate for the client machine and wait for the system to indicate that the client has stopped.

**Note:** When the command completes, the system displays a new prompt.

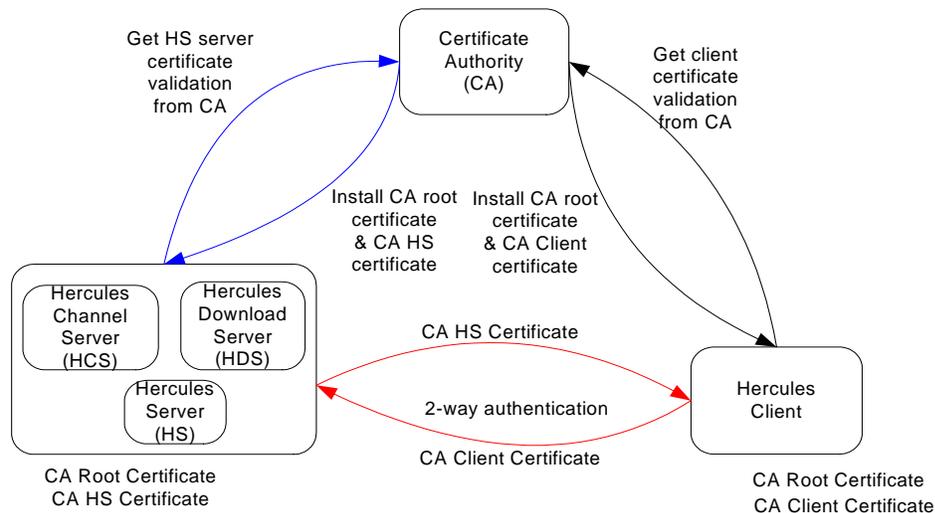
3. After the stop command completes, issue the start command appropriate for the client machine.
4. Verify that the start command has completed.

**Note:** When the command completes, the system displays a new prompt.

5. Repeat steps 1 to 4 at each machine where the Hercules client for UNIX, Linux, or Mac OS X is installed.

## Configuring Hercules to Use Certificates With 2-Way Authentication

The following graphic illustrates the process for 2-way authentication. The Hercules Server or Hercules Client independently requests from the CA a CA server or CA client certificate and the CA root certificate. The Hercules Server uses the CA root certificate to authenticate the Hercules Client's CA client certificate, and the Hercules Client uses the CA root certificate to authenticate the Hercules Server's CA server certificate. This allows the Hercules Server and Client to authenticate each others communications.



### Overview of Setting Up SSL and Certificates in Hercules (2-Way)

This section describes the following procedures for setting up SSL communication capability on Hercules and enabling SSL communications between the Hercules Server and the Hercules Administrator and Clients:

1. ["Requesting and Installing CA Certificates on the Hercules Server \(2-Way\)"](#) on page 4-15
2. ["Uninstall Hercules Clients for Microsoft Windows"](#) on page 4-3
3. ["Configure Hercules Clients for Microsoft Windows to use SSL \(2-Way\)"](#) on page 4-15
4. ["Configure Hercules Clients for UNIX to use CA Certificates \(2-Way\)"](#) on page 4-16
5. ["Configure Hercules URLs to Use HTTPS \(2-Way\)"](#) on page 4-16
6. ["Configure Clients for UNIX, Linux, and Mac OS X to Use HTTPS \(2-Way\)"](#) on page 4-16
7. ["Configure IIS to Require SSL Access and CA Client Certificates \(2-Way\)"](#) on page 4-17
8. ["Restart Hercules Clients for UNIX, Linux, and Mac OS X"](#) on page 4-17
9. ["Reinstall Hercules Clients for Microsoft Windows \(2-Way\)"](#) on page 4-18

### **Requesting and Installing CA Certificates on the Hercules Server (2-Way)**

To request and install CA certificates on the Hercules Server for two-way authentication, use the same procedures that you would use for one-way authentication (see ["Requesting and Installing CA Certificates on the Hercules Server \(1-Way\)"](#) on page 4-5).

### **Configure Hercules Clients for Microsoft Windows to use SSL (2-Way)**

In two-way certification, the Hercules Client needs SSL plus a unique CA client certificate, in addition to the CA root certificate. This process assumes that the Hercules Server is already configured to require client certificates, and to use `https://<certificate common name>` as the URL for clients. These steps provide some assistance to set up the client certificate portion of a secure Hercules installation:

1. ["Retrieve and Install the CA Root Certificate for Clients for Windows"](#) on page 4-5
2. Request CA client certificate from the CA.
3. Issue the CA client certificate.
4. To install the CA client certificate, from the Hercules Client desktop, browse to locate the certificate file and double-click on it to open the Certificate window.
5. Click **Install Certificate** to start the Certificate Import wizard. In the Welcome page, click **Next**.
6. Select **Place all certificates in the following store** and click **Browse**.
7. Select **Show physical stores**.
8. Select **Local Computer** under the personal Certificate Store.
9. Click **OK** and then click **Next**.
10. The wizard displays the settings. Click **Finish** to exit the wizard.

### Configure Hercules Clients for UNIX to use CA Certificates (2-Way)

Follow these steps to configure Hercules Clients for UNIX and Linux to use certificates in two-way authentication:

1. ["Enable SSL and HTTPS for Clients for UNIX, Linux and Mac OS X" on page 4-2.](#)

2. Generate a private key using RSA and/or DSA encryption methods.

*Note:* You can use OpenSSL for this. The key size is limited by the type of OpenSSL you are using.

RSA: `openssl genrsa -out <privkeyfile> <key-size>`

DSA: `openssl gendsa -out <privkeyfile> <key-size>`

RSA Example: `openssl genrsa -out privkey.pem 2048`

3. Generate a CA client certificate request by using the private key from step 2 and the following command:

`openssl req -new -key <privkeyfile> -out <certrequestfile>`

Example: `openssl req -new -key privkey.pem -out cert.req`

4. Submit CA client certificate request to CA.

5. Download issued CA client certificate to the Hercules Client.

6. Download CA root certificate to the Hercules Client.

7. To trust CA that signed the CA server certificate, issue this command:

`openssl x509 -hash -noout -in <CACertFile>`

where <CACertFile> is the name of the certificate file you downloaded in step 2.

8. Now issue this command, using the hash generated in step 7:

`ln -s <ca cert file> <hash>.0`

9. Add the following entries to `\opt\citadel\Hercules\hclient.conf`:

`certificate=<path where certificate is located>/<certfile>`

`private_key=<path where private key is located>/<privkeyfile>`

`ca_directory=<path where root CA certificates are located>`

### Configure Hercules URLs to Use HTTPS (2-Way)

This configuration is the same procedure as for 1-way authentication (see ["Configure Server URLs to Use HTTPS \(1-Way\)" on page 4-6](#)).

### Configure Clients for UNIX, Linux, and Mac OS X to Use HTTPS (2-Way)

This configuration is the same procedure as for 1-way authentication (see ["Modify Hercules Server URL from HTTP to HTTPS in hclient.conf" on page 4-10](#)).

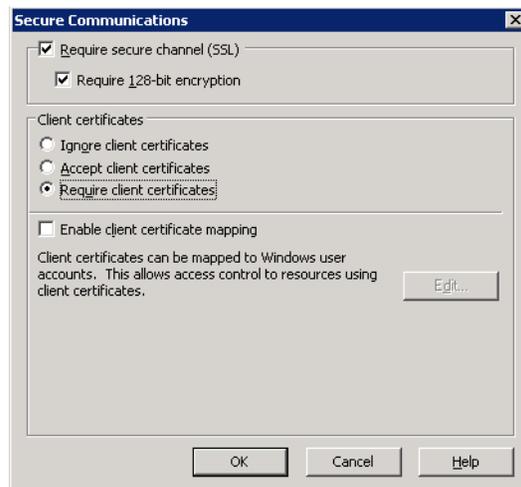
## Configure IIS to Require SSL Access and CA Client Certificates (2-Way)

This procedure uses Internet Services Manager to configure a virtual directory to require SSL for access. You can require the use of SSL for specific files, directories, or virtual directories. Hercules Clients must use the HTTPS protocol to access any such resource.

1. On the Hercules Server desktop, select Start > Administrative Tools > Internet Services Manager.
2. In the Internet Information Services (IIS) Manager window, expand your server name and then expand the **Web Sites** folder to display **Default Web Site**.
3. Locate **HerculesClientServices** in the list of folders. Right-click on it and then click **Properties**.
4. Click the **Directory Security** tab.
5. Under **Secure communications**, click **Edit**.
6. If you have Hercules Clients for Windows NT 4.0 in your network, you must first ["Configure 128-bit Encryption in Hercules Clients" on page 4-2](#).
7. Select the **Require secure channel (SSL)** and **Require 128-bit encryption** check boxes.

*Note:* Clients browsing to this virtual directory must now use HTTPS.

8. Select **Require client certificates**.



9. Click **OK**, and then click **OK** again to close the **Properties** dialog box.
10. Repeat steps 3-9 for **PatchRepository**.
11. Close the Internet Services Manager window. SSL with client certificates is now enabled in communications between the Hercules Server and Clients.

## Restart Hercules Clients for UNIX, Linux, and Mac OS X

If you are configuring SSL on an existing Hercules installation, you need to restart the Hercules Clients for UNIX, Linux, and Mac OS X (see ["Restart Hercules Clients for UNIX, Linux, and Mac OS X" on page 4-13](#)).

### Reinstall Hercules Clients for Microsoft Windows (2-Way)

If you are configuring SSL on an existing Hercules installation, Citadel recommends that you uninstall all Hercules Clients for Microsoft Windows (see "[Uninstall Hercules Clients for Microsoft Windows](#)" on page 4-3) before configuring SSL and reinstall them after configuring SSL. Follow these steps to install a client using CMS:

1. Launch the Hercules Administrator and select the desired Hercules Server.
2. Open the Manage Device Groups window, right-click on the desired device group, and then click **Install Hercules Client on Devices**.
3. In the Navigation pane, under **Operations**, click **Monitor device actions**.
4. Monitor the status of the devices until each of their status changes from **Queued** to **Succeeded**.

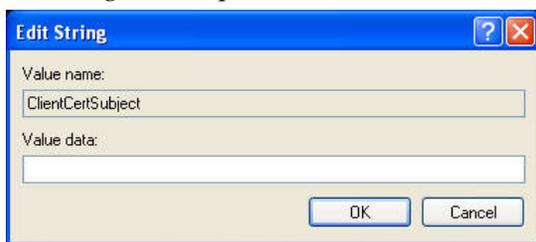
5. Repeat steps 1 to 4 for all groups in the server.

6. From the Hercules Client desktop, run `regedt32` to open the Registry Editor.

7. Expand `HKEY_LOCAL_MACHINE` to the **Client** folder:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citadel Security Software\Hercules\3.0\
Client
```

8. In the right-hand pane, double-click **ClientCertSubject** to open Edit String.



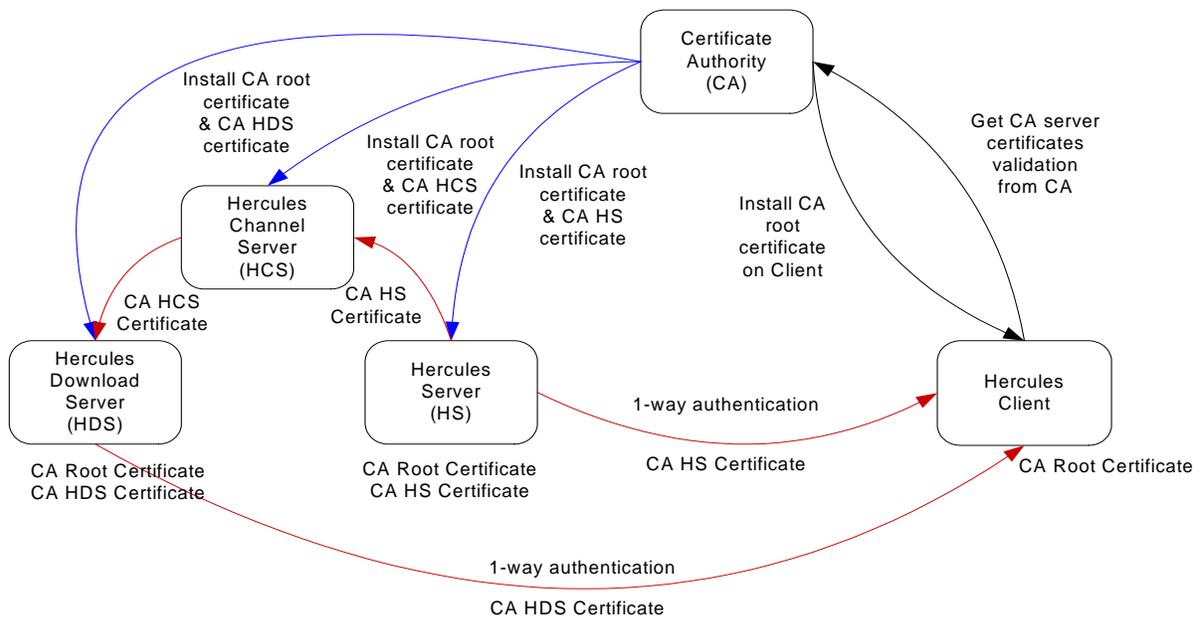
9. In the **Value Data** textbox, type the common name of the certificate.
10. Click **OK** and exit the Registry Editor.
11. Restart the Hercules Client service.

## Configuring SSL in Distributed Hercules Architecture

This section describes how to configure SSL in the Hercules system to use one-way and two-way authentication while operating in a distributed system, where all Hercules components communicate across the network. The same configuration procedures outlined for a standalone localhost mode apply to the distributed environment (see ["Configuring SSL in Hercules System Using Localhost Mode" on page 4-4](#)).

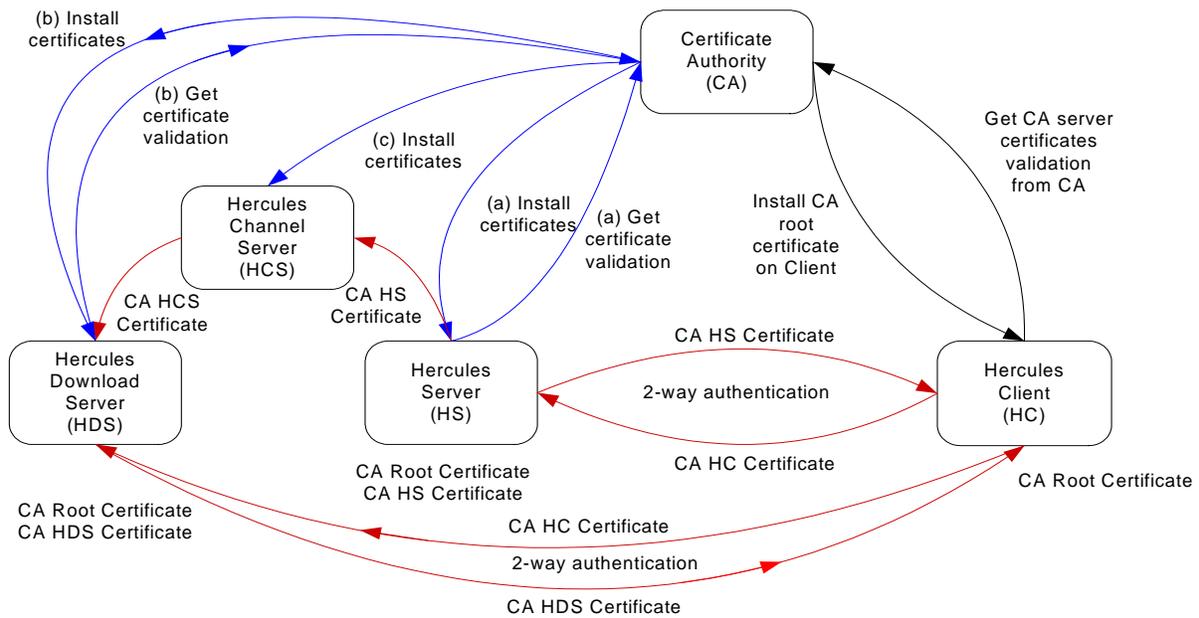
### One-Way Authentication in Hercules

The following graphic illustrates the process for 1-way authentication. All three Hercules servers request from the CA their own CA server certificate and the CA root certificate, while the Hercules Client independently requests the CA root certificate. The Hercules Client uses the CA root certificate to authenticate the CA server certificates of the Hercules Server (HS) and the Hercules Download Server (FDS). This allows the Hercules Client to authenticate the communication with the Hercules Server and the Hercules Download Server. The Hercules Administrator supports the same secure communications as the Hercules Client.



### Two-Way Authentication in Hercules

The following graphic illustrates the process for 2-way authentication. All three Hercules servers independently request from the CA their own CA server certificate and the CA root certificate. The Hercules Client requests independently from the CA a CA Client certificate and the CA root certificate. The Hercules Server and the Hercules Download Server use the CA root certificate to authenticate the Hercules Client's CA client certificate. The Hercules Client uses the CA root certificate to authenticate the CA server certificate of the Hercules Server or Hercules Download Server. This allows the Hercules Server, the Hercules Download Server, and the Hercules Client to authenticate each others communications.



## 5. Auditing All Hercules® Servers

---

### Setting up Audit Logging in Microsoft Windows

With Audit Logging, system administrators can audit local security events when Hercules uses a Microsoft Windows facility that is being audited, such as process tracking, policy changes, account logon events, system events, object access and directory services access. Audit Logging allows system administrators to track what a Hercules Server, Hercules Channel Server, or File Download Server is accessing and what a Hercules Client is doing on a client machine, based on Microsoft Windows audit capabilities. Audit Logging shows how remediation affects the Hercules Client or the Hercules Server, Hercules Channel Server, or File Download Server and policy changes on the Hercules Client.

Audit Policies determine which security events are logged into the Security log on the computer and are configured through Local Policies. The Security log is part of Event Viewer.

#### Microsoft TechNet and Help Resources

For detailed information on Local and Audit Policies and setting up Audit Logging on the machine where the Hercules Server, Hercules Channel Server, or File Download Server are installed, follow the instructions provided in "[Windows 2000 Common Criteria Security Configuration Guide](#)" on page R-1.

Additional guidance on Audit Logging is provided in the "[National Security Agency Recommendation Guides](#)" on page R-1.

For specific audit logging procedures, search Microsoft Help from your Windows desktop for the following and other related topics:

- Set up auditing of files and folders
- Specify files and folders to audit
- Viewing security logs
- Size of the security log

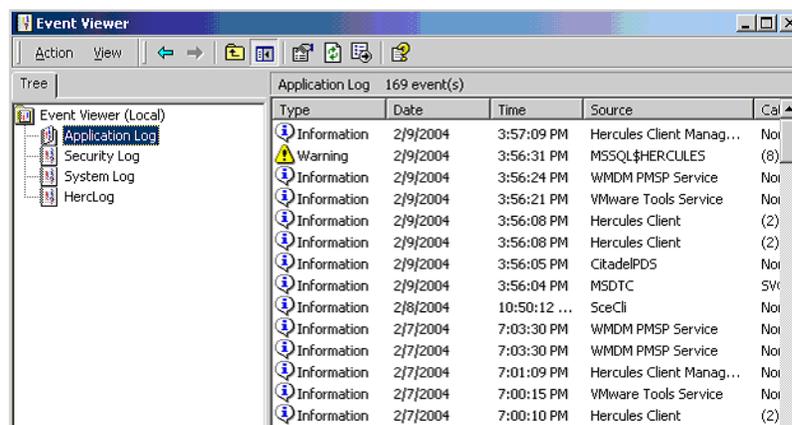
## Preventing Audit Trail Overflow

If you are auditing many objects, your Audit Log may fill up very quickly. To prevent audit trail overflow, Citadel recommends that you set all logs to overwrite after a certain size is reached.

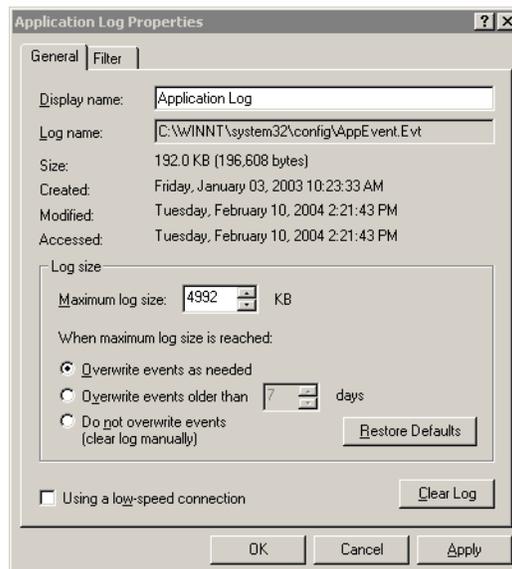
*Note:* When you install a Windows 2000 Server, the default is set to never overwrite the Audit Log.

### Prevent Audit Trail Overflow in Windows Server 2000

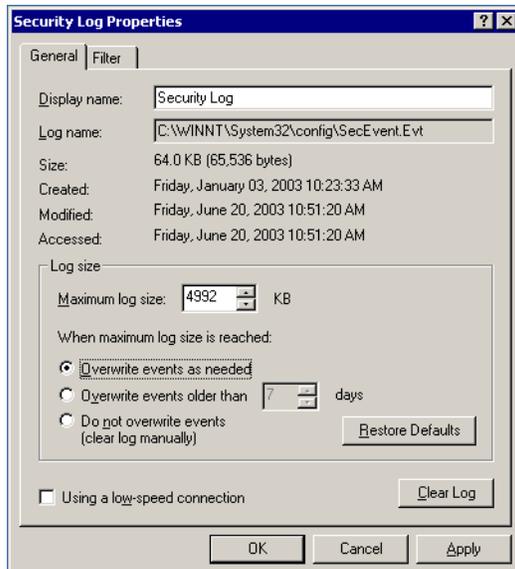
1. From any Hercules server desktop, select Start > Programs > Administrative Tools > Event Viewer.
2. In the Event Viewer window, select **Application Log** to display the logged events in the right-hand pane.



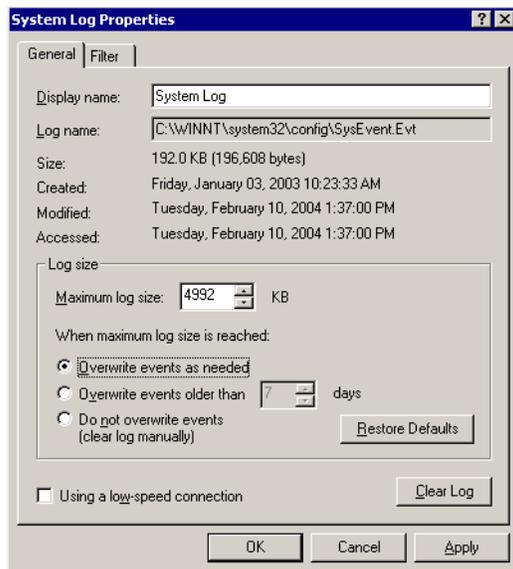
3. Right-click on **Application Log** and click **Properties** to display the Application Log Properties dialog box.
4. Select **Overwrite events as needed**. Change the **Maximum log size** to 4992 KB and click **Apply**.



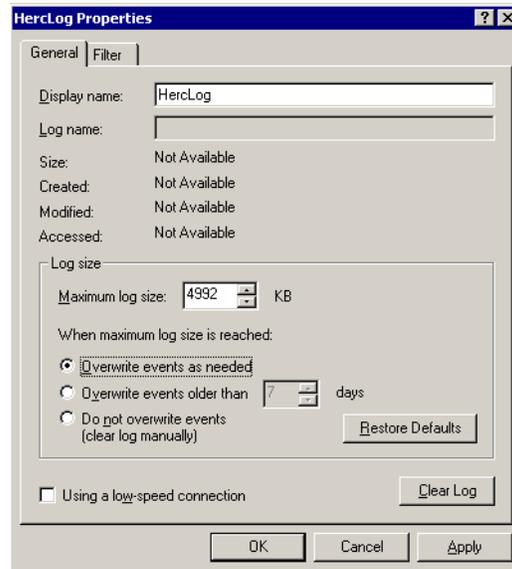
5. In the Event Viewer, right-click on **Security Log** and click **Properties**.
6. In the Properties dialog box, select **Overwrite events as needed**. Change the **Maximum log size** to **4992 KB** and click **Apply**.



7. In the Event Viewer, right-click on the **System Log** and click **Properties**.
8. In the Properties dialog box, select **Overwrite events as needed**. Change the **Maximum log size** to **4992 KB** and click **Apply**.



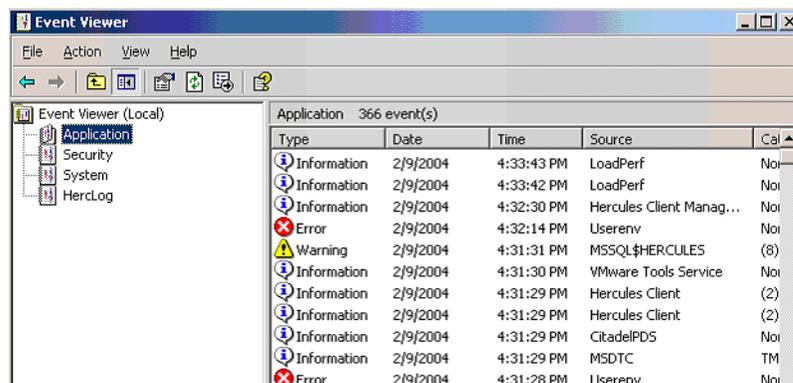
9. In the Event Viewer window, right-click on **HercLog** and click **Properties**.
10. In the Properties dialog box, select **Overwrite events as needed**. Change the **Maximum log size** to **4992 KB** and click **Apply**.



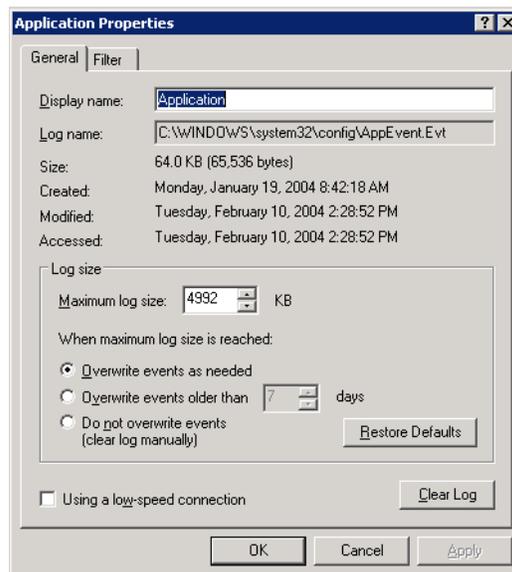
11. Close the Event Viewer.

### Prevent Audit Trail Overflow in Windows 2003 Server

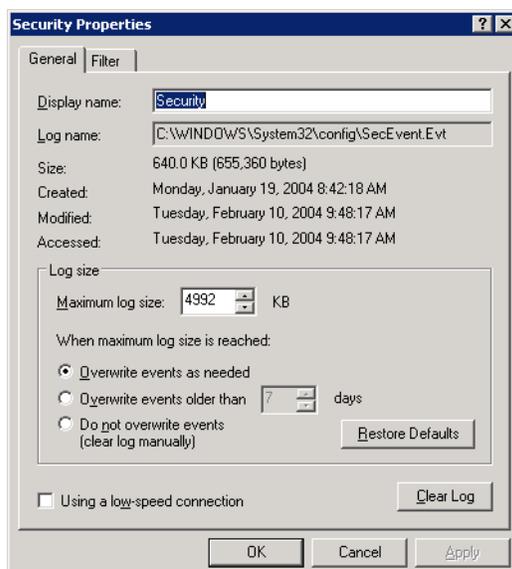
1. From any Hercules server desktop, select Control Panel > Administrative Tools > Event Viewer.
2. In the Event Viewer window, select **Application Log** to display the logged events in the right-hand pane.



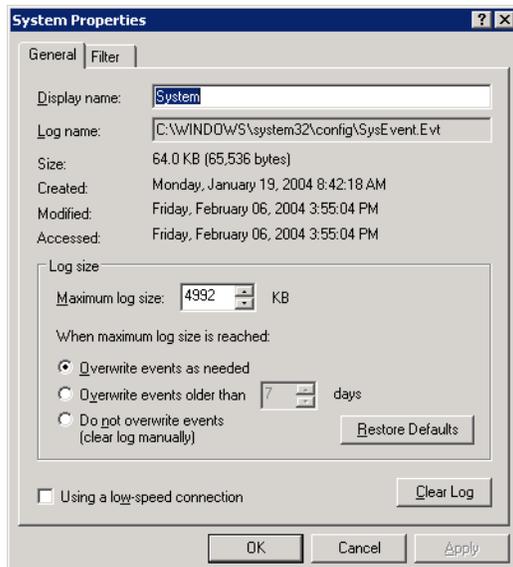
3. Right-click on **Application Log** and click **Properties** to display the Application Log Properties dialog box.
4. Select **Overwrite events as needed**. Change the **Maximum log size** to **4992** KB and click **Apply**.



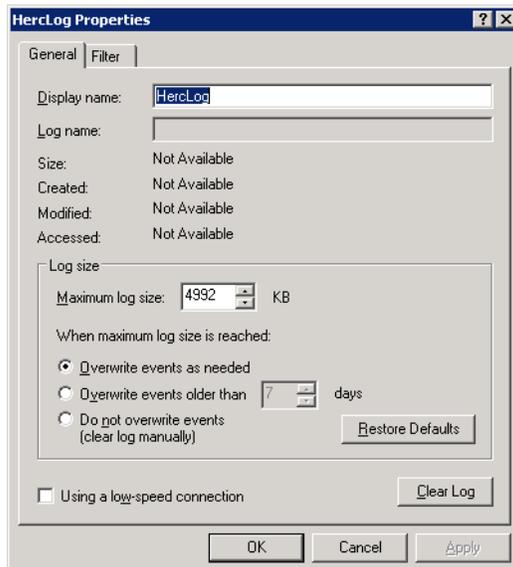
5. In the Event Viewer, right-click on **Security Log** and click **Properties**.
6. In the Properties dialog box, select **Overwrite events as needed**. Change the **Maximum log size** to **4992** KB and click **Apply**.



7. In the Event Viewer, right-click on the **System Log** and click **Properties**.
8. In the Properties dialog box, select **Overwrite events as needed**. Change the **Maximum log size** to **4992 KB** and click **Apply**.



9. In the Event Viewer window, right-click on **HercLog** and click **Properties**.
10. In the Properties dialog box, select **Overwrite events as needed**. Change the **Maximum log size** to **4992 KB** and click **Apply**.



11. Close the Event Viewer.

## Auditing All Types of Hercules Servers

This section describes audit logging of Microsoft IIS 5.0, Hercules Software registry key, Hercules working directories and Hercules databases for Hercules Servers, Hercules Channel Server, and File Download Servers.

### Configuring Microsoft Internet Information Services Audit Logging

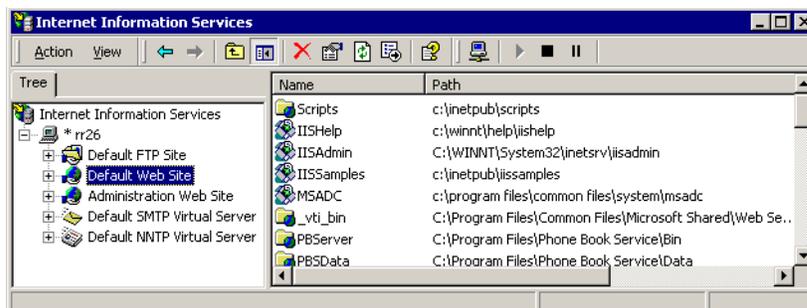
You should configure IIS audit logging for the Hercules Server, Hercules Channel Server, and File Download Server.

**WARNING:** IIS logging on a heavily loaded Hercules Server can degrade performance.

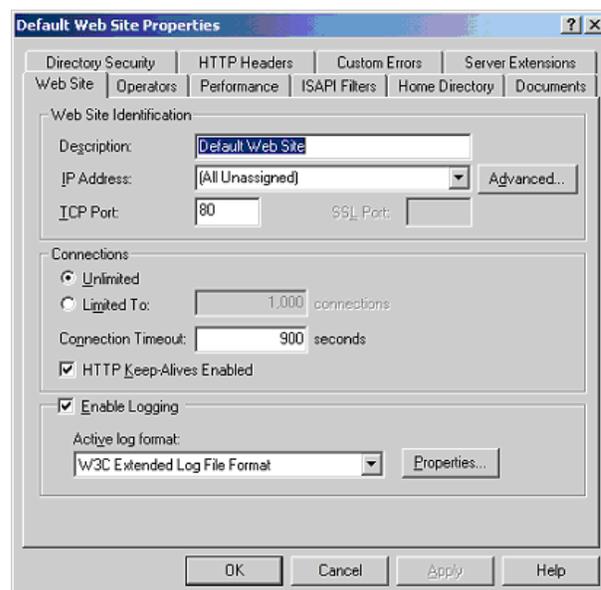
#### Configure IIS 5.0 Audit Logging in Windows 2000 Server

Follow these steps to configure IIS 5.0 Audit Logging in Windows 2000 Server:

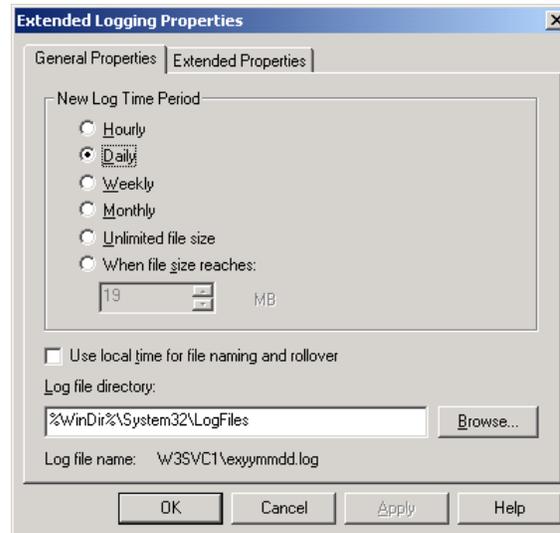
1. From your desktop, select Start > Programs > Administrative Tools > Internet Services Manager. The Internet Information Services window displays.
2. In the left-hand pane, expand the server to display the **Default Web Site** folder and right-click on it. Select **Properties**.



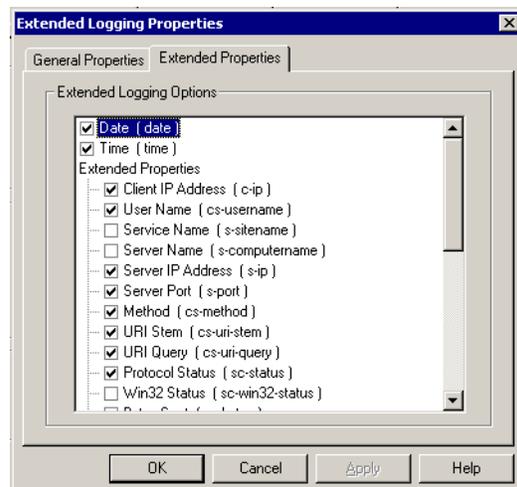
3. In the Default Web Site Properties dialog box, verify that the **Enable Logging** check box is selected. Click on the **Properties** button.



4. In the Extended Logging Properties dialog box, click on the **General Properties** tab.
5. Verify that all the logging property settings are correct for your site. If you make changes, click **Apply**; otherwise click **OK**.



6. Click on the **Extended Properties** tab. Verify that the check boxes of the following items are selected for logging, as shown below. In addition, verify that **User Agent** (not shown) is also selected.:

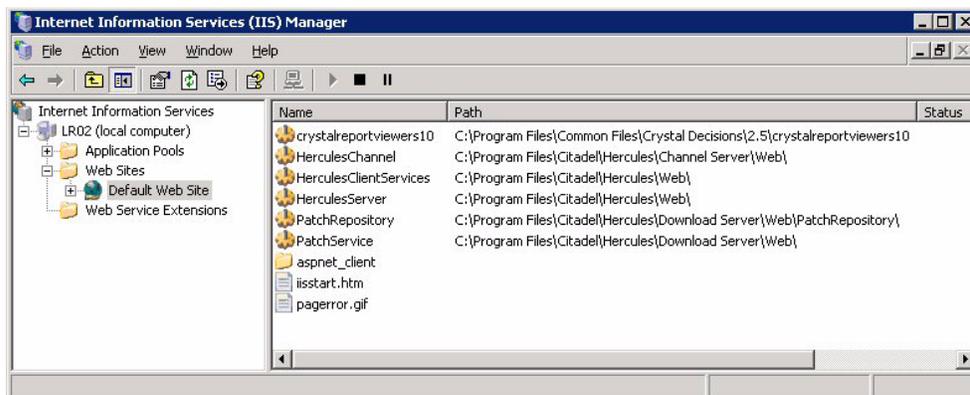


7. Click **OK** to save your changes.
8. Stop and restart the World Wide Web Publishing Service to update your logging settings.

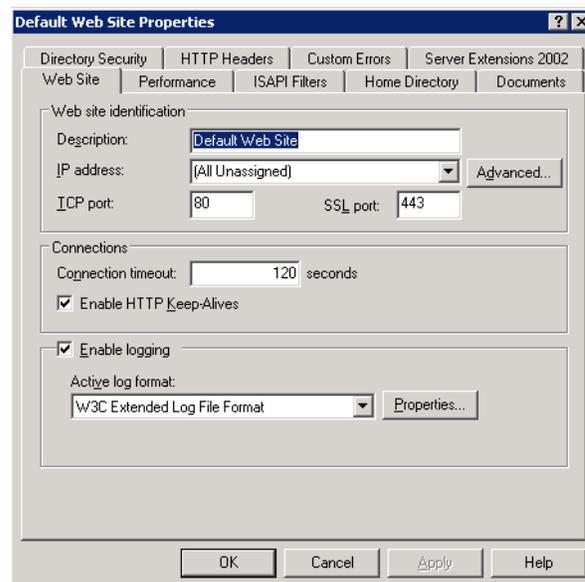
## Configure IIS 6.0 Audit Logging in Windows Server 2003

The procedure for auditing IIS 6.0 is different than for IIS 5.0. Follow these steps to audit IIS 6.0 on the Windows Server 2003 where the Hercules Server, Hercules Channel Server, or File Download Server is installed:

1. From any Hercules server desktop, select Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager.
2. Expand **Web Sites** folder and right-click on **Default Web Site**. Select **Properties**.

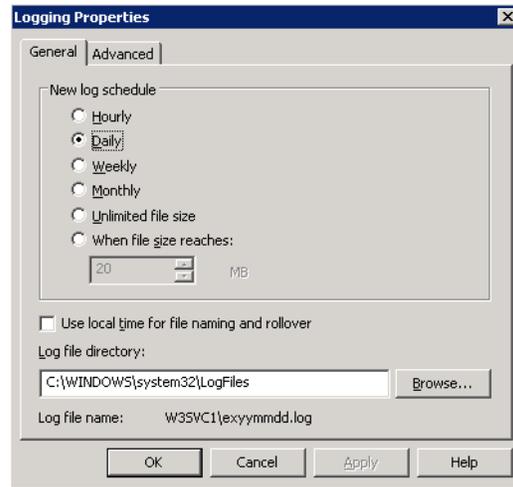


3. In the Default Web Site Properties dialog box, click the **Web Site** tab.
4. Verify that the **Enable Logging** check box is selected and that the **Active log format** displayed is **W3C Extended Log File Format**. If you make changes, click **Apply**.

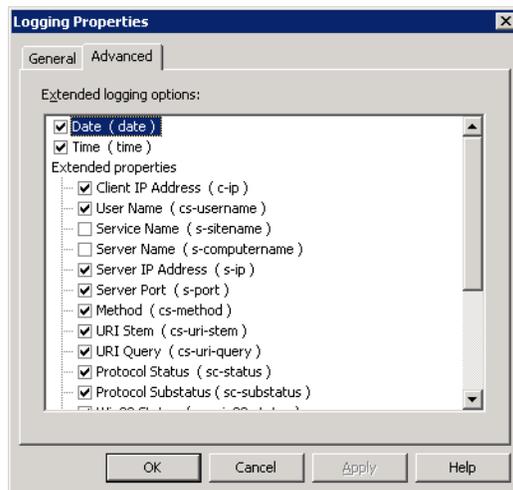


5. Click the **Properties** button and then click the **General** tab.

- Verify that all the logging property settings are correct for your site. If you make changes, click **Apply**; otherwise, click **OK**.



- Click on the **Advanced** tab. Verify that the check boxes for the following extended logging options are selected. In addition, **Win32 Status** and **User Agent** check boxes (not shown) should also be selected. If you make changes, click **Apply**; otherwise click **OK**.



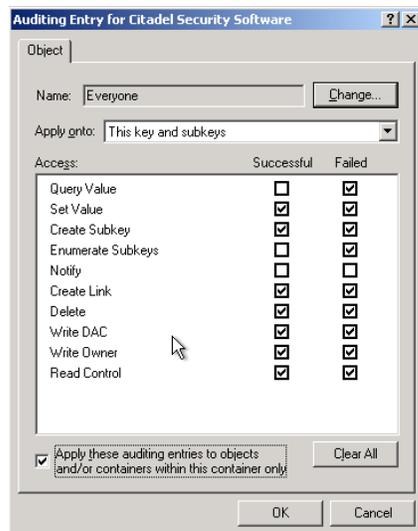
## Enabling Auditing of Hercules Software Registry Key

You should configure audit logging of the Hercules software registry key for the Hercules Server, Hercules Channel Server, and File Download Server.

### Enable Auditing of Hercules Software Registry Key in Windows 2000

1. From any Hercules server desktop, run regedt32 to open the Registry Editor.
2. Expand the following key:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Citadel Security Software
3. From the **Security** menu, click **Permissions**.
4. In the Permissions for Citadel Security Software dialog box, click **Advanced**.
5. In the Access Control Settings for Citadel Security Software dialog box, click the **Auditing** tab.
6. Click **Add** and select **Everyone** from your local machine.
7. The Auditing Entry for Citadel Security Software dialog box displays. Select the settings identified in the dialog box below.

**Note:** The system will create two audit entries.



8. Select the check box to apply auditing entries to child objects and enable propagation of inheritable audit entries.
9. Click **OK** three times to close all dialog boxes.

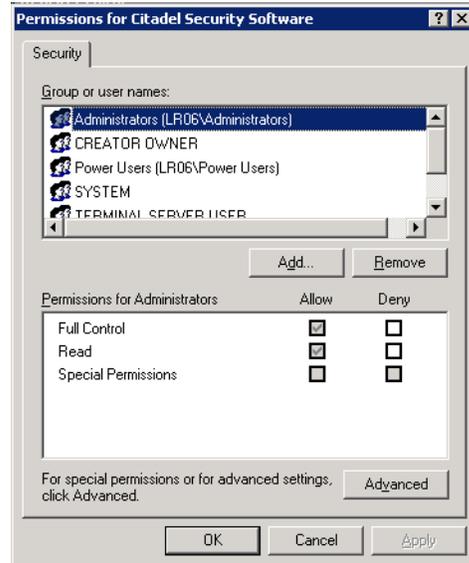
## Enable Auditing of Hercules Software Registry Key in Windows 2003

1. From any Hercules server desktop, run regedt32 to open the Registry Editor.

2. Expand the following key:

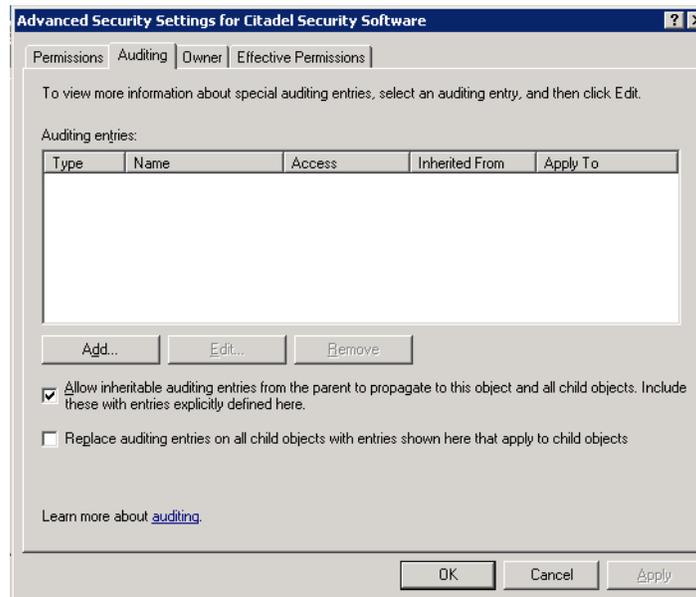
HKEY\_LOCAL\_MACHINE\SOFTWARE\Citadel Security Software

3. From the **Edit** menu, click **Permissions**.

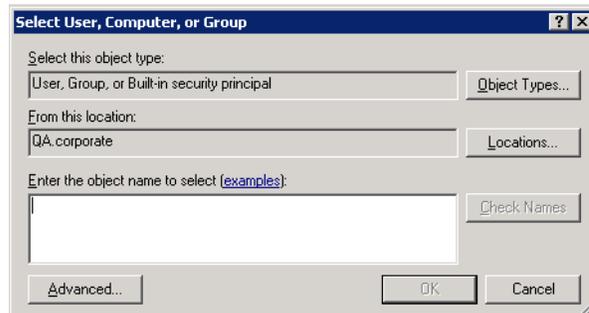


4. In the Permissions for Citadel Security Software dialog box, click **Advanced**.

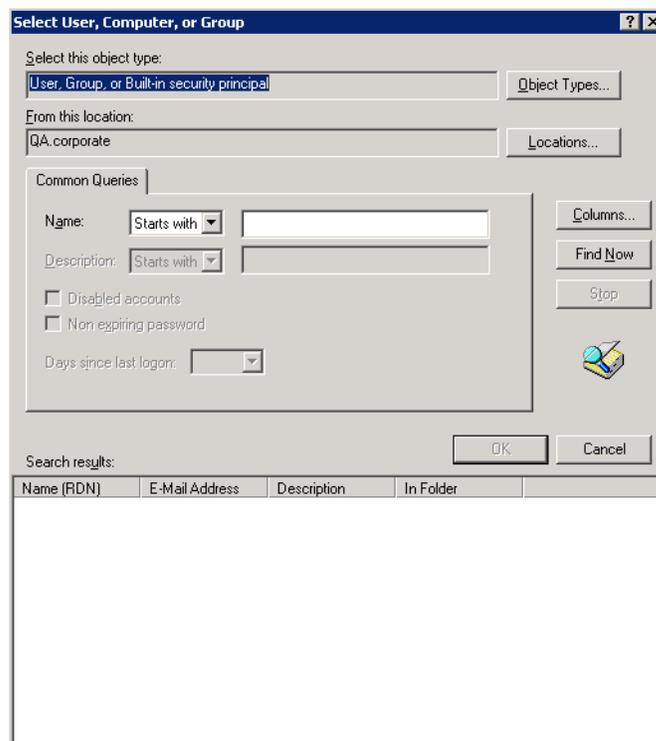
5. In the Advanced Security Settings dialog box, click the **Auditing** tab.



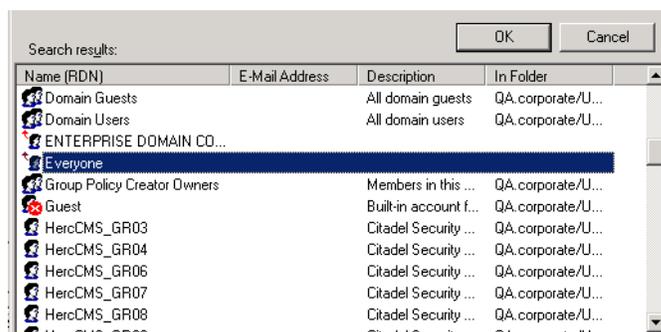
6. Click **Add** to display the Select User, Computer, or Group dialog box.



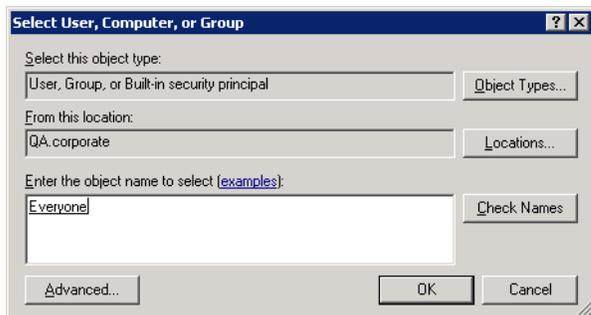
7. Click **Advanced** to expand the dialog box.



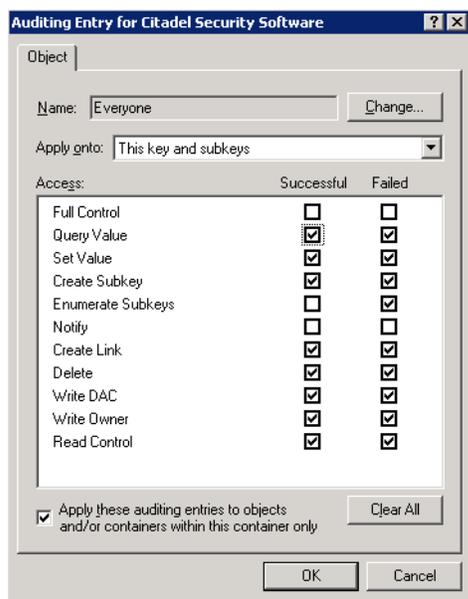
8. Click **Find Now** to display the list of users in the **Search results** bottom pane.



9. Select **Everyone** and click **OK**. **Everyone** is now displayed in the Object name bottom pane.



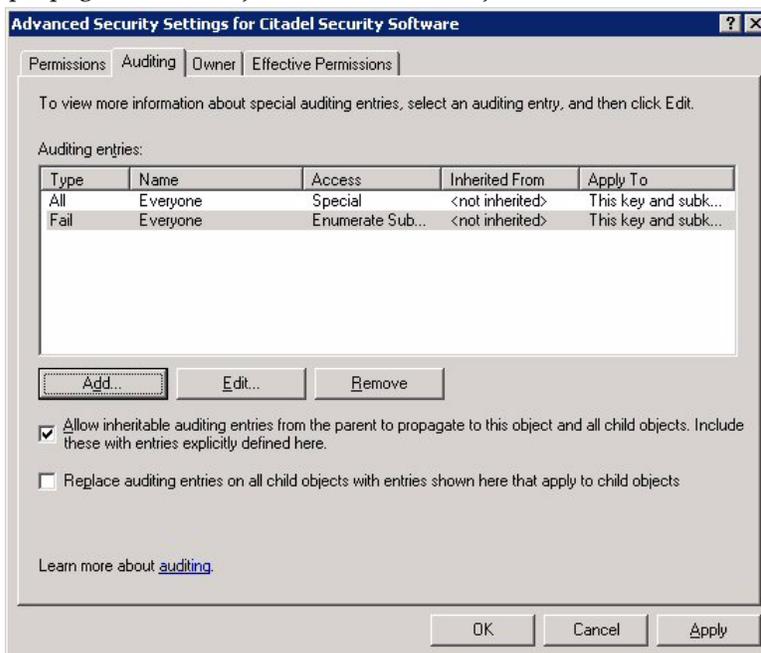
10. Click **OK**. The Auditing Entry for Citadel Security Software dialog box displays. Select the settings identified in the dialog box below.



11. Select the check the box to apply auditing entries to objects and/or containers within this container only. Click **OK**.

*Note:* The system will create two audit entries

12. Check the checkbox to allow inheritable auditing entries from the parent to propagate to this object and all child objects. Then click **OK**.



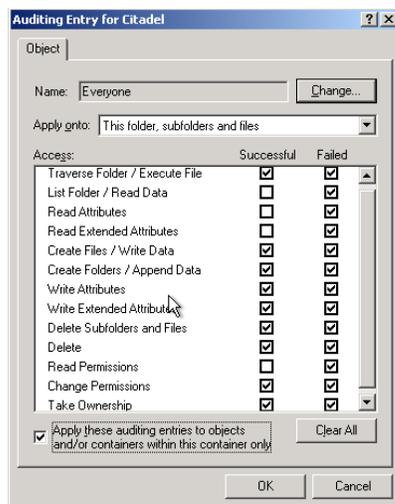
## Enabling Auditing of Hercules Working Directory

You should configure audit logging of the Hercules working directory for the Hercules Server, Hercules Channel Server, and File Download Server.

### Enable Auditing of Hercules Working Directory in Windows 2000

This procedure is very similar to ["Enable Auditing of Hercules Software Registry Key in Windows 2000" on page 5-11.](#)

1. From any Hercules server desktop, browse to the following directory:  
`<Install Drive>:\Program Files\Citadel`
2. Right-click on the **Citadel** folder and click **Properties**.
3. Click on the **Security** tab.
4. Click on the **Advanced** button.
5. Click on the **Auditing** tab.
6. Click on the **Add** button.
7. The Auditing Entry for Citadel dialog box displays. Select the settings identified in the dialog box below.

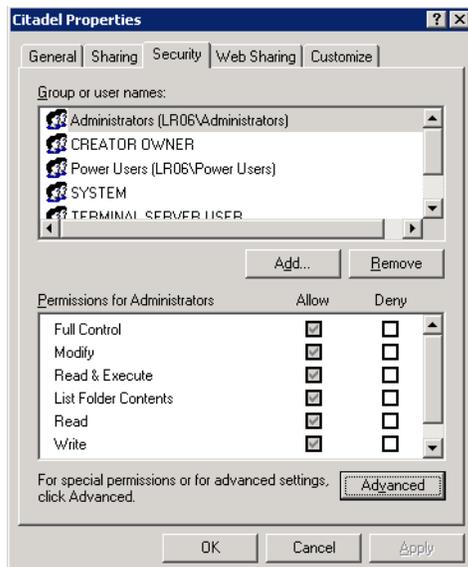


8. Select the check the box to apply auditing entries to child objects and enable propagation of inheritable audit entries.
9. Click **OK** three times to close all dialog boxes.

## Enable Auditing of Hercules Working Directory in Windows 2003

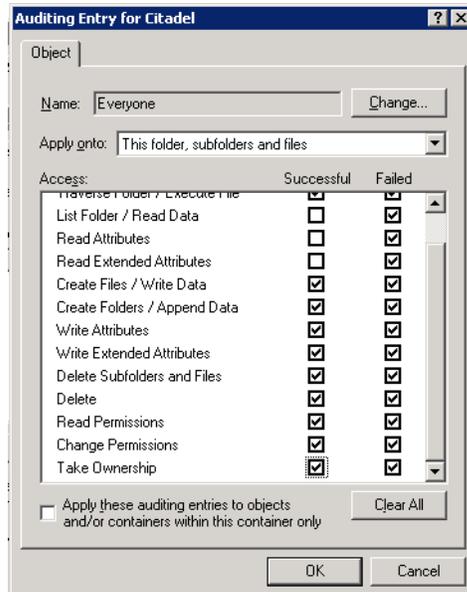
This procedure is very similar to ["Enable Auditing of Hercules Software Registry Key in Windows 2003" on page 5-12.](#)

1. From any Hercules server desktop, browse to the following directory:  
`<Install Drive>:\Program Files\Citadel`
2. Right-click on **Citadel** folder and click **Properties**.
3. In the Citadel Properties dialog box, click on the **Security** tab.



4. Click on the **Advanced** button to display the Advanced Security Settings dialog box.
5. Click on the **Auditing** tab and then click **Add**.
6. In the Select User, Computer, or Group dialog box, click **Advanced** to expand it.
7. Click **Find Now** to display the list of users in the **Search results** bottom pane.
8. Select **Everyone** and click **OK**. **Everyone** is now displayed in the object name list in the bottom pane of the Select User, Computer or Group dialog box.

- Click **OK**. The Auditing Entry for Citadel dialog box displays. Select the settings identified in the dialog box below.



- Select the check the box to apply auditing entries to child objects and enable propagation of inheritable audit entries.  
*Note:* The system will create two audit entries.
- Click **OK** to close all dialog boxes.

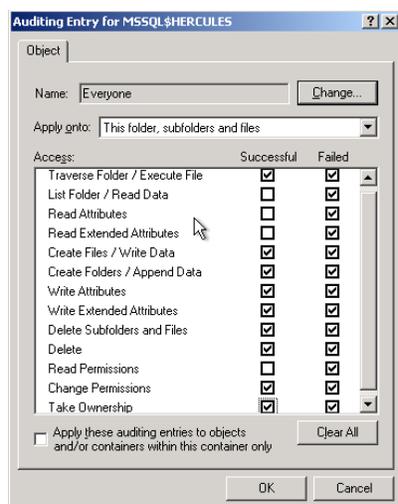
## Enabling Auditing of Hercules Databases

You should configure audit logging of all Hercules databases in the Hercules Server, Hercules Channel Server, and File Download Server.

### Enable Auditing of Hercules Database in Windows 2000

This procedure is very similar to ["Enable Auditing of Hercules Working Directory in Windows 2000" on page 5-16](#).

1. From any Hercules server desktop, browse to the following directory:  
`<Install Drive>:\Program Files\MSSQL Server\MSSQL$Hercules`
2. Right-click on **MSSQL\$Hercules** folder and click **Properties**.
3. Click on **Security** tab.
4. Click on the **Advanced** button.
5. Click on the **Auditing** tab.
6. Click on the **Add** button.
7. The Auditing Entry for MSSQL\$Hercules dialog box displays. Select the settings identified in the dialog box below.



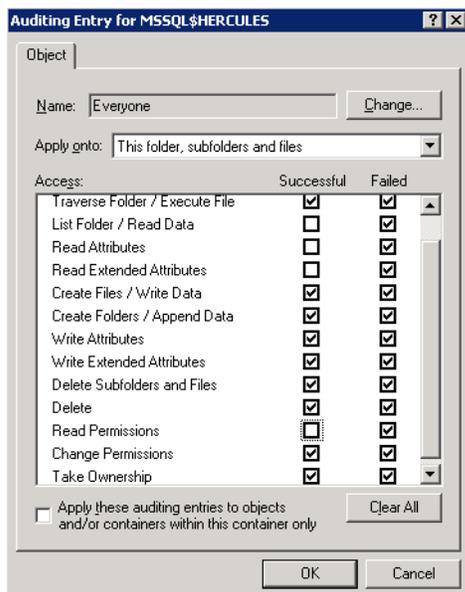
8. Select the check the box to apply auditing entries to child objects and enable propagation of inheritable audit entries.
9. Click **OK** three times to close all dialog boxes.

### Enable Auditing of Hercules Database in Windows 2003

This procedure is very similar to ["Enable Auditing of Hercules Working Directory in Windows 2003" on page 5-17](#).

1. From any Hercules server desktop, browse to the following directory:  

```
<Install Drive>:\Program Files\Microsoft SQL Server\MSSQL$Hercules
```
2. Right-click on the **MSSQL\$Hercules** folder and click **Properties**.
3. In the MSSQL\$Hercules Properties dialog box, click on the **Security** tab.
4. Click on the **Advanced** button to display the Advanced Security Settings dialog box.
5. Click on the **Auditing** tab and then click **Add**.
6. In the Select User, Computer, or Group dialog box, click **Advanced** to expand it.
7. Click **Find Now** to display the list of users in the Search results list in the bottom pane.
8. Select **Everyone** and click **OK**. **Everyone** is now displayed in the object name list in the bottom pane of Select User, Computer, or Group dialog box.
9. Click **OK**. The Auditing Entry for MSSQL\$Hercules dialog box displays. Select the settings identified in the dialog box below.



10. Select the check the box to apply auditing entries to child objects and enable propagation of inheritable audit entries.
11. Click **OK** to close all dialog boxes.

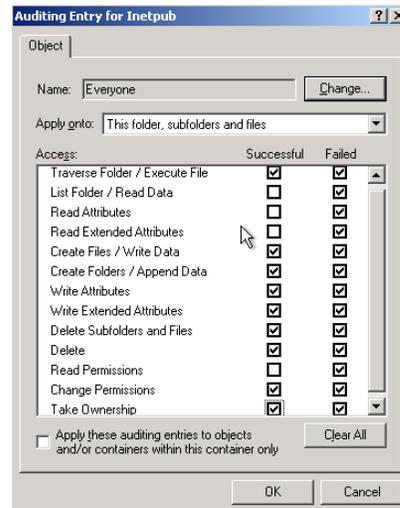
## Enabling Auditing of Hercules Public Directory on Web Server

You should configure audit logging of the Hercules public directory on the web server for the Hercules Server, Hercules Channel Server, and File Download Server.

### Enable Auditing of Public Directory on Web Server in Windows 2000

This procedure is very similar to ["Enable Auditing of Hercules Working Directory in Windows 2000" on page 5-16](#).

1. From any Hercules server desktop, browse to the following directory:  
`<Install Drive>:\inetpub`
2. Right-click on the **inetpub** folder and click **Properties**.
3. Click on the **Security** tab.
4. Click on the **Advanced** button.
5. Click on the **Auditing** tab.
6. Click on the **Add** button.
7. The Auditing Entry for Inetpub dialog box displays. Select the settings identified in the dialog box below:

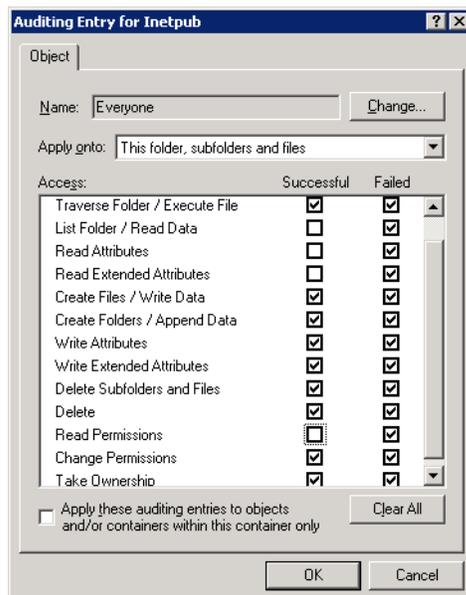


8. Select the check the box to apply auditing entries to child objects and enable propagation of inheritable audit entries.
9. Click **OK** three times to close all dialog boxes.

### Enable Auditing of Public Directory on Web Server in Windows 2003

This procedure is very similar to ["Enable Auditing of Hercules Working Directory in Windows 2003" on page 5-17](#).

1. From any Hercules server desktop, browse to the following directory:  
`<Install Drive>:\inetpub`
2. Right-click on the **inetpub** folder and click **Properties**.
3. In the inetpub Properties dialog box, click on the **Security** tab.
4. Click on the **Advanced** button to display the Advanced Security Settings dialog box.
5. Click on the **Auditing** tab and then click **Add**.
6. In the Select User, Computer, or Group dialog box, click **Advanced** to expand it.
7. Click **Find Now** to display the list of users in the **Search results** list in the bottom pane.
8. Select **Everyone** and click **OK**. **Everyone** is now displayed in the object name list in the bottom pane of Select User, Computer, or Group dialog box.
9. Click **OK**. The Auditing Entry for Inetpub dialog box displays. Select the settings identified in the dialog box below:



10. Select the check the box to apply auditing entries to child objects and enable propagation of inheritable audit entries.
11. Click **OK** to close all dialog boxes.

---

# Appendix A: Security Best Practices

---

## Security Environment

This section includes recommended best practices for Hercules installation environment, secure operations, and secure communication.

### Controlled Environment Installation

The Hercules Server is an integral component of network security and you should install it where production servers are located. Installing the Hercules Server in a controlled environment such as a data center or server room provides greater stability and security.

The Hercules Server should be used with other best practices for security, including:

- System hardening and configuration
- Securing the Hercules installation to specific user accounts
- Physical security access controls
- Perimeter security (firewalls)

### Maintaining Secure Operation of Hercules in the Event of Failure

#### Configure System Failure and Recovery Options

To maintain a secure operating system, Microsoft provides you with the following options to configure the actions that the operating system will take in the event of a system crash or other system error:

- Write event to the System log
- Send an administrative alert
- Dump system memory to a file for later debugging
- Automatically restart the computer

For detailed procedures on how to configure these actions, see ["How to Configure System Failure and Recovery Options in Windows"](#) on page R-2.

#### Configure Audit Trail Overflow

If you are auditing many objects, your Audit Log may fill up very quickly. To prevent audit trail overflow, Citadel recommends that you set all logs to overwrite after a certain size is reached or a certain time period. For detailed procedures, see ["Preventing Audit Trail Overflow"](#) on page 5-2.

## V-Flash Server Secure Communication

Hercules provides one-way authentication from the V-Flash server to the V-Flash client located in your Hercules Server. The V-Flash client connects with Citadel's V-Flash server through an HTTPS connection in order to download vulnerabilities and signatures from the V-Flash server.

To provide one-way authentication, the V-Flash server obtains a certificate from the VeriSign Certificate Authority; the V-Flash client does not use a certificate. The V-Flash server access is not restricted and requires no validation. The URL of the V-Flash server is fixed in the V-Flash client and cannot be changed by any user.

## Password and Access Controls

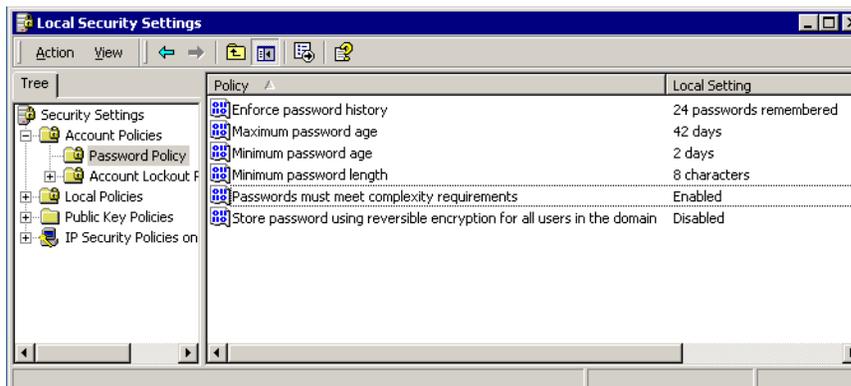
This section discusses password security requirements and recommendations.

### Password Security Requirements

The following are the settings required for EAL 3 compliance for securing Hercules Administrator passwords:

- Minimum password length shall be eight characters in length.
- Minimum password age (length of time before changing a password) should be two days.
- Maximum password age should be 42 days.
- Setting entitled **Enforce password history** should be 24.
- Setting entitled **Password must meet complexity requirements** shall be enabled.
- Setting entitled **Store password using Reversible Encryption for all users in the domain** shall be disabled.

To configure the password security settings, from the Hercules Server desktop, select Start > Control Panel > Administrative Tools > Local Security Policy and expand Security Policies/Account Policies/Password Policy.



## Changing CMS User Password on Hercules Server

You should change the CMS password as often as required by the security best practices of your organization. If you change your account password you will also need to change your CMS password. CMS is usually configured during the Hercules installation but it can be done later using the same procedure described here; for additional details on configuring CMS, see the *Hercules Installation Guide* and the *Hercules User's Guide*. This can be done using only a common local account that is valid on the machines you plan to manage.

To change the CMS User Password:

1. From the command prompt on the Hercules Server, locate the **Services** folder under the Hercules installation. The default Hercules Server installation path is:

```
C:\Program Files\Citadel\Hercules\Services
```

2. To install CMS, type the following command at the DOS prompt:

```
clientmgrservice -install
```

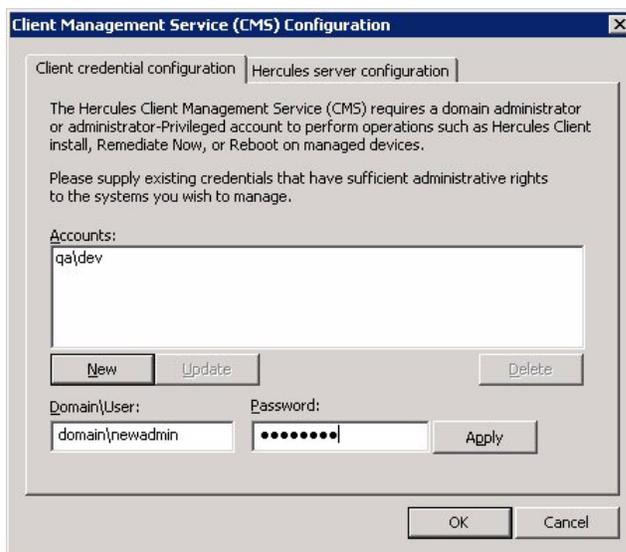
For example:

```
C:\Program Files\Citadel\Hercules\Services>clientmgrservice -install_
```

**Note:** An alternative procedure is to bring up the Run dialog box. Click the Windows **Start** button, select **Run**, enter the following in the textbox, and then click **OK**.

```
C:\Program Files\Citadel\Hercules\Services\clientmgrservice -install
```

3. Click **New** to enable the fields for entering credentials. Read the requirements at the top of the dialog box. For **Domain\User**, enter the domain and username separate by a backslash(\). For **Password**, type the corresponding password. Then click **Apply** to add the new credentials to the account list. Repeat as needed, then click **OK**.



## Configuring Clients for UNIX, Linux, and Mac OS X for Sudo Access

In the Hercules system, sudo allows users defined in the `sudoers` file to have temporary root access to run CMS commands (install/uninstall, start/stop, remediate, and reboot). Although sudo is optional, Citadel recommends that you use sudo for security reasons. Before configuring devices to allow sudo access for Hercules Clients for UNIX, Linux, and Mac OS X, you will first need to install the sudo utility (version 1.6.7 or later). Then you will need to modify the `sudoers` configuration file with the `visudo` editor to allow the user account sudo access for each CMS action.

**Note:** To facilitate configuration, you can create and use a generic Hercules user account and copy the `sudoers` configuration file to all devices that need sudo.

After configuring Hercules Clients to use sudo access, you can configure the Hercules Administrator to allow sudo access for those clients (for detailed procedures, see page 4-6 in the *Hercules User's Guide*):

- Configure sudo access for a particular Hercules Server
- Allow sudo access for all devices in a device group or individual devices

---

# Appendix B: Services to Shut Down

---

## Level 1 Basic Shutdown of Unnecessary Services

The following list shows what services are currently shut down by the Level 1 remedy in Windows Server 2000 and Windows 2003 Server. This list is subject to change at any time.

It is strongly recommended that the Hercules Server machine be installed with a static IP address, but the Level 1 template will not shut down the DHCP Client on your Hercules Server machine. If your machine is configured with a dynamic address, you should reconfigure it with a static address and shut down the DHCP Client manually.

**Table 1: Basic Shutdown of Unnecessary Services**

Operating System	Service
Both	Alerter
Both	Automatic Updates
Both	Background Intelligent Transfer Service
Both	Clipboard
Both	Messenger
Both	FTP Publishing Service
Windows Server 2000	Internet Connection Sharing
Both	Netmeeting Remote Desktop Sharing
Both	Routing and Remote Access
Both	Simple Mail Transfer Protocol (SMTP)
Both	Wireless Configuration
Both	SQLServerAgent
Both	MSSQLServerADHelper
Both	Telnet

## Level 2 Moderate Shutdown of Unnecessary Services

The following is a list of unnecessary services that are currently shut down by the Level 2 remedy in Windows Server 2000 and Windows 2003 Server.

**Table 1: Moderate Shutdown of Unnecessary Services**

Operating System	Service
Windows Server 2003	Application Layer Gateway Service
Both	Application Management
Both	Computer Browser
Both	Distributed File System
Both	Distributed Link Tracking Client
Both	Distributed Link Tracking Server
Windows Server 2003	Error Reporting Service
Windows 2000 Server	Fax Service
Both	File Replication
Windows Server 2003	Help and Support
Windows Server 2003	Human Interface Device Access
Windows Server 2003	IMAPI CD_Burning COM Service
Both	Indexing Service
Windows Server 2003	Internet Connection Firewall (ICF)/ Internet Connection Sharing (ICS)
Both	Intersite Messaging
Windows 2000 Server	IPSEC Policy Agent
Windows Server 2003	IPSEC Services
Both	Kerberos Key Distribution Center
Both	License Logging Service
Windows Server 2003	Microsoft Software Shadow Copy Provider
Both	Network DDE
Both	Network DDE DSDM
Windows Server 2003	Network Location Awareness (NLA)
Both	Performance Logs and Alerts
Windows Server 2003	Portable Media Serial Number Service
Both	Print Spooler
Windows 2000 Server	QoS RSVP

**Table 1: Moderate Shutdown of Unnecessary Services (Continued)**

<b>Operating System</b>	<b>Service</b>
Both	Remote Access Auto Connection Manager
Both	Remote Access Connection Manager
Windows Server 2003	Remote Desktop Help Session Manager
Both	Remote Procedure Call (RPC) Locator
Both	Remote Registry Service
Both	Removable Storage
Windows Server 2003	Resultant Set of Policy Provider
Windows 2000 Server	RunAs Service
Windows Server 2003	Secondary Logon
Windows Server 2003	Shell Hardware Detection
Both	Smart Card
Windows 2000 Server	Smart Card Helper
Windows Server 2003	Special Administration Console Helper
Both	SQLAgent\$HERCULES
Both	Task Scheduler
Both	Telephony
Windows Server 2003	Terminal Services Session Directory
Windows Server 2003	Themes
Windows Server 2003	Upload Manager
Windows Server 2003	Volume Shadow Copy
Windows Server 2003	WebClient
Windows Server 2003	Windows Image Acquisition (WIA)
Both	Windows Time
Windows Server 2003	WinHTTP Web Proxy Auto-Discovery Service



---

# References

---

References to third party vendor documentation and web sites are subject to change without notice. Alternate paths are provided to facilitate finding the sources in the event the link becomes disabled.

## General

### **Hercules Level 1 and Level 2 Security Configuration Guide Patch List**

Download from <https://hercules.citadel.com/docs/seclevel.htm>

### **National Security Agency Recommendation Guides**

<http://www.nsa.gov/snac/>

### **Windows 2000 Common Criteria Security Configuration Guide**

<http://www.microsoft.com/technet/security/topics/issues/w2kccscg/default.aspx>

Or, navigate in your Internet browser from <http://www.microsoft.com> to TechNet Home > Security > Security Topics > Standards, Regulations, and Government Issues > Windows 2000 Common Criteria Secure Configuration Guide

### **Windows Server 2003 Security Guide**

<http://www.microsoft.com/technet/security/prodtech/win2003/default.aspx>

Or, navigate in your Internet browser from <http://www.microsoft.com> to TechNet Home > Security > Product and Technology Security Centers > Windows Server 2003

### **Security Innovations in Windows Server 2003**

<http://www.microsoft.com/windowsserver2003/techinfo/overview/secinnovation.aspx>

## Microsoft Internet Information Services

### **Internet Information Services 5.0 Lockdown Tool**

<http://www.microsoft.com/technet/security/tools/locktool.aspx>

Download from <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=DDE9EFC0-BB30-47EB-9A61-FD755D23CDEC>

### **Guide to Secure Configuration and Administration of Microsoft IIS 5.0**

<http://nsa2.www.conxion.com/win2k/guides/w2k-14.pdf>

## CA Certificates and SSL

### Certificates

<http://www.microsoft.com/technet/security/topics/crypto/certs.msp>

Or, navigate in your Internet browser from <http://www.microsoft.com> to TechNet Home > Security > Security Topics > Cryptography and Secure Communications > Introduction to Certificates.

### Guide to Secure Configuration and Administration of Windows 2000 Certificate Services

Download from <http://nsa2.www.conxion.com/win2k/guides/w2k-12.pdf>

### How to Set Up SSL on a Web Server

Download from <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/SecNetHT16.asp>

Or, navigate in your Internet browser from <http://www.microsoft.com> to MSDN Home > MSDN Library > .NET Development > .NET Security > Building Secure ASP.NET Applications > How To Set Up SSL on a Web Server.

### How to Set Up Client Certificates

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/SecNetHT17.asp>

Or, navigate in your Internet browser from <http://www.microsoft.com> to MSDN Home > MSDN Library > .NET Development > .NET Security > Building Secure ASP.NET Applications > How To Set Up Client Certificates

### Step-by-Step Guide to Setting Up a Certification Authority

<http://www.microsoft.com/windows2000/techinfo/planning/security/casetupsteps.asp>

### Microsoft Certificate Services Using Windows Server 2003

[http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/standard/proddocs/en-us/sag\\_cs\\_topnode.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/standard/proddocs/en-us/sag_cs_topnode.asp)

Or, navigate in your Internet browser from <http://www.microsoft.com/> to TechNet Home > Products & Technologies > Windows Server 2003 > Product Documentation > Standard Edition Help > Security > Public Key Infrastructure > Certificate Services

## System Failure

### How to Configure System Failure and Recovery Options in Windows

<http://support.microsoft.com/default.aspx?scid=kb;en-us;307973>

Or, navigate in your Internet browser to <http://support.microsoft.com> and search for the Knowledge Base Article 307973.