Certificate Based Access Control (CBAC) Operation and User Guide

4 April, 2003

Law Enforcement/Corrections Program Support

CBAC
Operation and User Guide

Security Statement: This document contains no classified information, nor shall any classified information be added to this document.

Distribution Statement: Distribution authorized to U.S. Government agencies and their contractors. Other requests for this document shall be referred to Space and Naval Warfare Systems Command, Washington, D.C. 20363-5100.

Contents

Figures

1 INTRODUCTION

Certificate Based Access Control (CBAC), formerly known as Palladium, is a complete privilege management software system, to address the need for a central access control system. CBAC technology allows state and local criminal justice agencies to share information with complete confidence and control. CBAC is a platform-independent access control system that enables agencies to share information while maintaining control of their data. Applications incorporating CBAC allow agencies to control their data based on role definitions and individual user attributes found in digital certificates. By utilizing policy-defined rule-sets, agencies transcend the traditional username, login access control paradigm. Administrators create and maintain rule-sets through a web-based graphical user interface. Creating or modifying access rule-sets is simple, enabling agencies to stay up-to-date with policy decisions.

Benefits:

- Permits need-to-know access to sensitive information
- Allows agencies to define policy-based rule-sets for access control
- Enables distributed access control for a federation of systems
- Enhances private networks by enabling varying levels of access
- Decreases administrative time

Features:

- Platform independent
- Configurable for an existing PKI infrastructure or set-up with internally signed certificates
- Standard interfaces - RMI, CORBA, and XML Socket interfaces
- Easy to use web-based administrators page
- Rule-set templates
- Rapid implementation with no impact to end-users.

There are three primary components to the CBAC system: Certificate Access Determination and Evaluation Server (CADES), Certificate Access Preparation and Review Tool (CAPR), and the Rules Database (RulesDB).

System Administrators create and modify system parameters using the web-based CAPR system. The system parameters include: RuleSets, trusted Certificate Authorities (CAs) and other system parameters. The system administrators then push the configurations to the CADES servers and re-initialize the CADES server. The CADES servers can either be local or remote.

Client Applications format access control requests using the CADES application program interface (API) and request are processed by the CADES server and are responded to using the format of the CADES API.

The CADES server will broker access control queries for an integrated client application. Upon initialization the CADES server loads the RuleSets, trusted CAs, and any additional information specified in the database.

CADES processes the access requests in accordance to the access control policy that has been defined with the CAPR subsystem. The GRANT/DENY rule set for the CADES server are loaded at initialization or when new RuleSets or pushed and cycled into memory. CADES generates responses as defined in the API.

CBAC is capable of functioning on any operating system containing a Java Virtual Machine. When using CBAC with the ISAPI filter, the system must be installed on Windows NT machine with Microsoft's Internet Information Server (IIS).

2 INSTALLATION, CONFIGURATION AND MAINTENANCE

The CBAC system supports (1) administration and management of certificate-based access control rules outside the context of any particular system, site, or application and (2) a standard, simple mechanism to allow an application that is presented a digital certificate to obtain the access permissions associated with that certificate. By utilizing digital certificates the system permits administrators to create access control guidelines based on all "self-describing" fields found within X509 Certificates, such as Agency, Location, Common Name, and X509 Extension information. Once defined, a user can be associated with a list of either granted or denied resources ranging from database records, to web pages. This section describes the procedures to install, start, operate, restart, and stop the CBAC solution.

Minimum Requirements

Hardware Requirements

All hardware requirements will depend on the amount of expected demand of the CBAC system. The general rule of thumb is to consider the CBAC requirements equal to an entry-level web server.

- Computer - Server class CPU
- RAM - 256 megabytes (MB) of RAM recommended minimum. All CBAC processing is done in active memory. Therefore, additional memory will improve performance.
- Hard Disk - 2 GB free hard disk space. Disk space is used for supporting applications and for log files.

Software Requirements

- JDK 1.3-compatible operation system (OS). If using Windows NT 4.0, service patch 6 (SP6) is a minimum.
- Microsoft IIS must also be fully patched and accept SSL connections and employ https://
- Tomcat
- InstantDB (or some database to support rule set storage)
- Unzipping application

Functional Requirements

The CBAC system needs an existing security infrastructure. This infrastructure can be a simple username password challenge pair, a Lightweight Directory Server (LDAP), or as complex as a public key infrastructure (PKI). The CBAC system also needs a business policy rule set that will be applied to the RuleSet database. The default rule is to DENY ALL.

Installation

Installation Instructions

For installation instructions please follow the guidance of the CBAC Operation Instructions Document.

Configuration

For configuration instructions please follow the guidance of the CBAC Operation Instructions Document.

Maintenance

Monitoring for System Errors

System Administrators should monitor logs for system errors. Additionally they must rotate system logs off the system. For log files Browse to [PALLADIUM HOME]\log

Shutdown

When the system is running as an application on Windows it can be shutdown simply by closing the application window. When running as a server on Windows, the Control Panel > Services tool should allow the system to be stopped and started. On Linux the application must be killed using process ids.

Backup

CBAC does not require any special backup procedures. Although it is recommended to backup the [PALLADIUM HOME] directory.

Parameters and System Configuration

CADES

The CADES property file found at [PALLADIUM_HOME]\properties\cades.properties. Listed below is a complete list of the supported properties and a description of their purpose (* parameters are server implementation specific):

- *cades.rmi.name – The name by which the Cades Server object will be bound to the rmi registry.
- *cades.socket.port – The port on which the socket server will accept connections
- cades.name – A user defined name for this CADES server. Must be unique, used by the CAPR system.
- cades.provider -- Provider used for parsing of Certificate. Unless specifically attempting to use a new Java Provider use default: 'com.templar.crypt.provider.Provider'
- cades.logfile – The folder to which the log files should be saved. Within this folder the system will create a subdirectory entitled certificates that will contain all logged user certificates, stored by serial number.
- cades.extractor – The class to use for CertificateExtraction. Unless specifically developed, use default: 'com.templar.rbcf.CertificateExtraction'
- cades.extractor.propertyfile – The property file for the extractor defined above, default is: [PALLADIUM_HOME] \properties\CertificateExtractor.properties
- cades.rulesdb.address – The fully qualified jdbc name for the Rules Database. Example: 'jdbc:mysql://200.100.100.100/cadesdb'. Please see database jdbc driver to verify format.
- cades.rulesdb.loginspec – Full path to an encrypted file containing username and password for access to the rules database.
- cades.rulesdb.driver – Fully qualified classname for the JDBC driver to be used to access the Rules Database. Example: 'sun.jdbc.odbc.JdbcOdbcDriver'
- cades.application.[i] – A list of all the applications and hosts that this CADES will support. Each application takes the format name@host, where * can be used as a wildcard for either name or host.

CAPR

CAPR has multiple parameters that can be configured. These parameters are all found in [PALLADIUM_HOME]\properties\caprres.properties:

- capr.context – The Tomcat context under which the CAPR application JSPs can be found
- capr.extractor -- The class to use for CertificateExtraction. Unless specifically developed, use default: 'com.templar.rbcf.CertificateExtraction'
- capr.extractor.propertyfile -- The property file for the extractor defined above, default is: [PALLADIUM_HOME] \properties\CertificateExtractor.properties
- capr.database.driver -- Fully qualified classname for the JDBC driver to be used to access the Rules Database. Example: 'sun.jdbc.odbc.JdbcOdbcDriver'
- capr.database.host -- The fully qualified jdbc name for the Rules Database. Example: 'jdbc:mysql://200.100.100.100/cadesdb'. Please see database jdbc driver to verify format.
- capr.search.criteria – The search criteria that will be used to locate applicable CADES servers within this RulesDatabse. Default: online=1
- permission.class.[i] – A list of all the Permission classes that are supported by CAPR. For a permission to be supported it must be added to this list or manually be entered into CAPR each time a new Rule is created. Example: 'java.io.FilePermission'

3 OPERATING PROCEDURES

The CBAC system supports (1) administration and management of certificate-based access control rules outside the context of any particular system, site, or application and (2) a standard, simple mechanism to allow an application that is presented a digital certificate to obtain the access permissions associated with that certificate. By utilizing digital certificates the system permits administrators to create access control guidelines based on all "self-describing" fields found within X509 Certificates, such as Agency, Location, Common Name, and X509 Extension information. Once defined, a user can be associated with a list of either granted or denied resources ranging from database records, to web pages.

The purpose of the Operating section is to describe the operating procedures to load, start, operate, restart, and stop the CBAC solution.

Starting CBAC

The first page in CBAC you see is the CAPR login screen found at http://localhost:8080/capr

Tomcat and the appropriate CADES must be running to access this page.

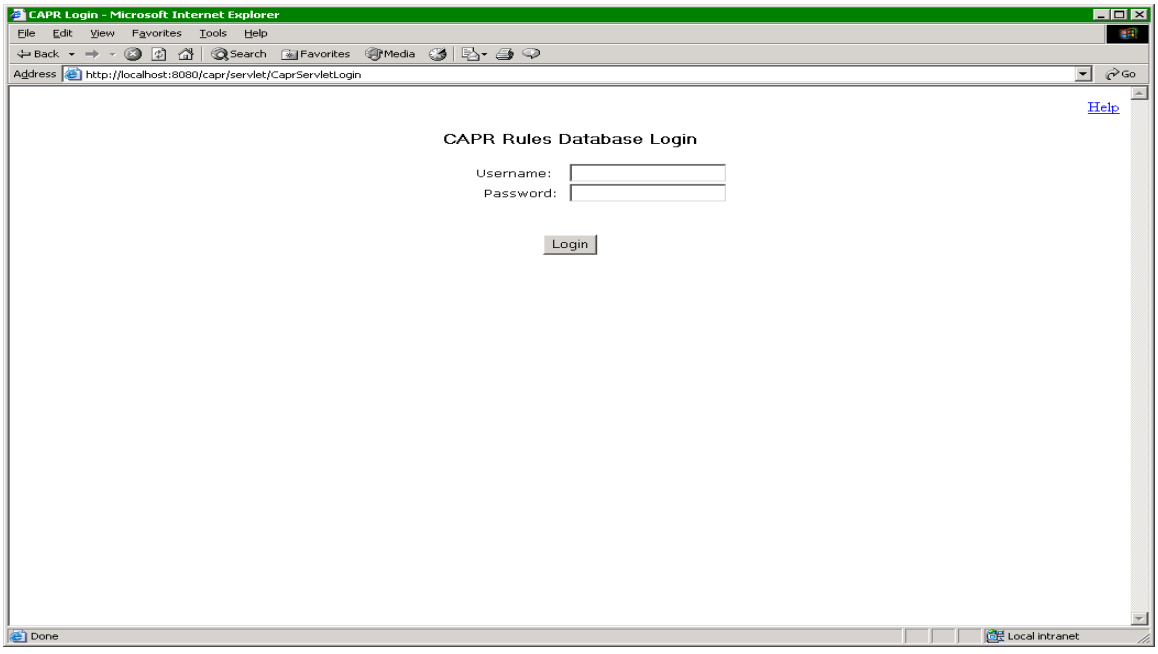

Figure 3-1. CAPR Rules Database Login Screen

This is the login page for the CAPR System. You must enter your username and password. Improper logins will return you to this page.

1. Enter your assigned username used to login to the Rules Database.

   Note: The Username field is case sensitive.

2. Enter your password.

   Note: The Password field is case sensitive.

3. Once all the fields are entered properly, click the **Login** button. This will bring you to the CAPR Main page.

The CAPR Main Page

All administrative tools and functions for CBAC are accessed from the CAPR Main page. The page contains two main sections. The RuleSet table at the top of the page lists the primary attributes of each RuleSet in the Rules Database. The Other Tools menu at the bottom contains links to other CBAC functions and tools.

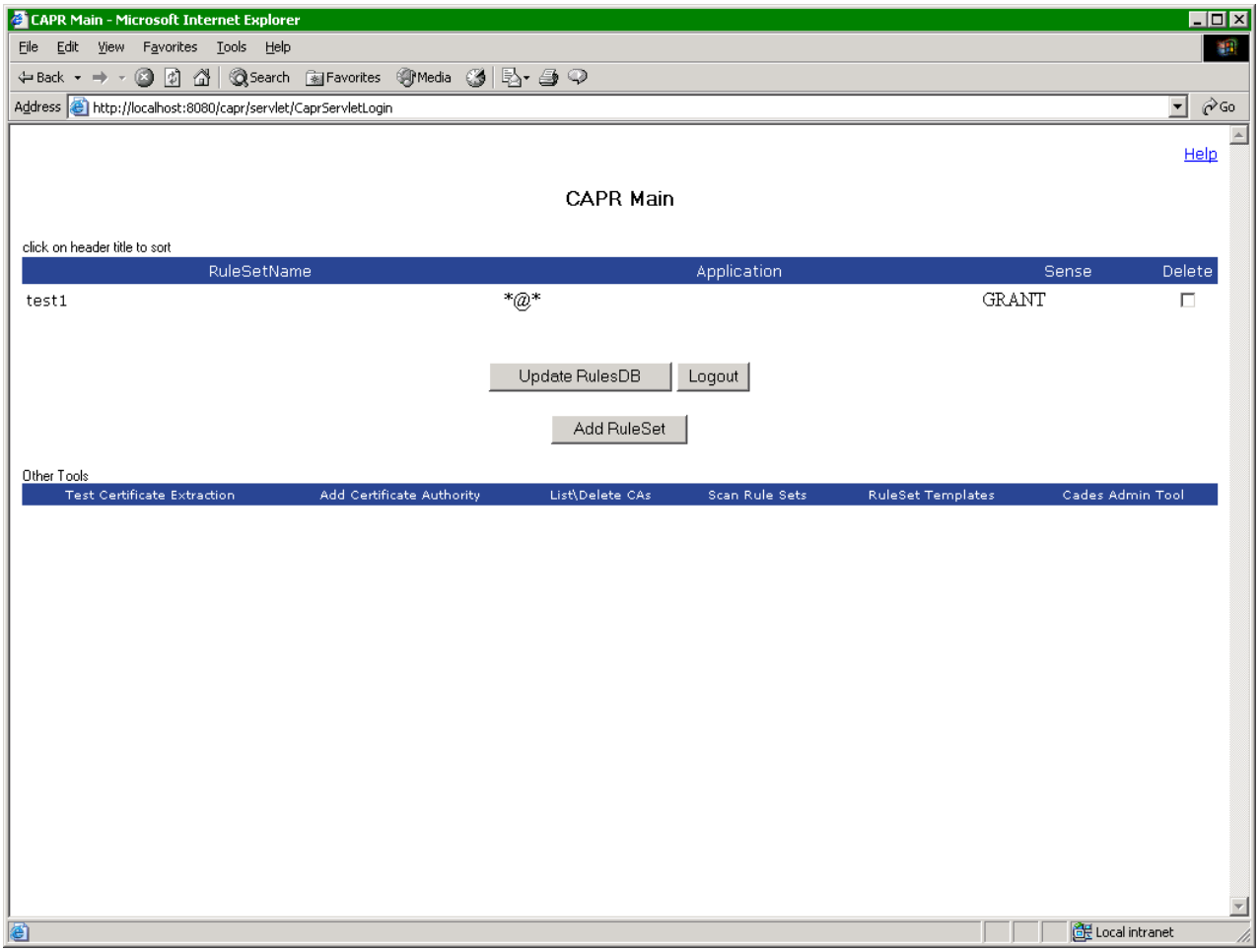

Figure 3-2. CAPR Main Page

RuleSet Table

The principal feature of the page is a table listing the three primary attributes of each RuleSet in the Rules Database. A RuleSet is a conglomeration of Permission and Access Controls to restrict access to sensitive resources. The values in this table are not editable. To change any of the RuleSet Properties, the administrator must select a RuleSet by clicking on its RuleSet Name and make any changes in the RuleSet Detail window. The table can be sorted based on any of the following three primary attributes by clicking on the linked column title name.

RuleSet Name

This is a unique name given to each of the RuleSets by the administrator. This field is not used by the Cades system except for logging. By clicking on any of the names the user will bring up the detail view for that particular RuleSet. Once a RuleSet has been modified "(mod)" appears after the name.

Application

The application to which this RuleSet applies. Specified as application@host. If no host is specified the RuleSet is assumed to apply to all hosts on a given application. Wildcards are supported for both the application and host names.

Sense

Either GRANT or DENY, describing whether the client is granted or denied permission if the Rule evaluates to true. In addition to the table listing the RuleSets and their attributes there are a number of actions an administrator can perform:

Update RulesDB Button

Updates the Rules Database with all changes to the RuleSets (those specified with "(mod)" after their name) and deletes all RuleSets whose Delete column has been marked.

NOTE: Changes made to RuleSets take effect only when the Rules Database is updated. Logging out without clicking the Update RulesDB button will result in the loss of all changes

Logout Button

Logs the user out without altering the Rules Database. All changes to the RuleSets will be lost.

Add RuleSet Button

Opens a blank RuleSet detail page, allowing the user to specify all of the attributes of a new RuleSet.

Other Tools

Additional CBAC tools are provided on this menu on the CAPR Main page and are described below.

Test Certificate Extraction

Allows the user to test the extraction of a Base-64 encoded certificate. Resulting display shows parsed fields using system assigned names

Add Certificate Authority

Allows a user to enter a Base-64 encoded certificate authority into CBAC's trusted root store.

List / Delete CAs

Lists all of the Trusted Certificate Authorities (CA) within the CA Database sorted by their Subject Distinguished Name fields. In addition Certificate Authorities may be removed from CBAC's trusted root store.

Scan Rule Sets

This is a tool used by administrators to verify that no rules exist that aren't being used. The system permits the creation of Grant rules, which may never be checked if their permissions are implied by another Deny RuleSet. This system scans checks for any such rules and displays them in a chart.

Rule Set Templates

This shows a list of Rule Set Templates that can be used as a basis for other users to create their own Rule Sets. This feature is specifically designed for users who do not have much knowledge of Rule Sets and Certificate access. This feature allows the user to create a basic outline for a Rule Set defining Rules as needed and save this as a template. Other users can export this template and use it for their own applications. RuleSet Templates are created by clicking the **Add RuleSet** button on the CAPR Main Page. Set the name and any Rules and Permissions that apply and save the Rule Set as a template by clicking the Create As Template button.

CADES Administrative Tool

This tool allows an administrator to force specified Query Servers to reload rules from the Rules Database.

Adding a RuleSet

1. From the CAPR Main page, click the **Add RuleSet** button.
2. The Rule Set Detail screen displays.

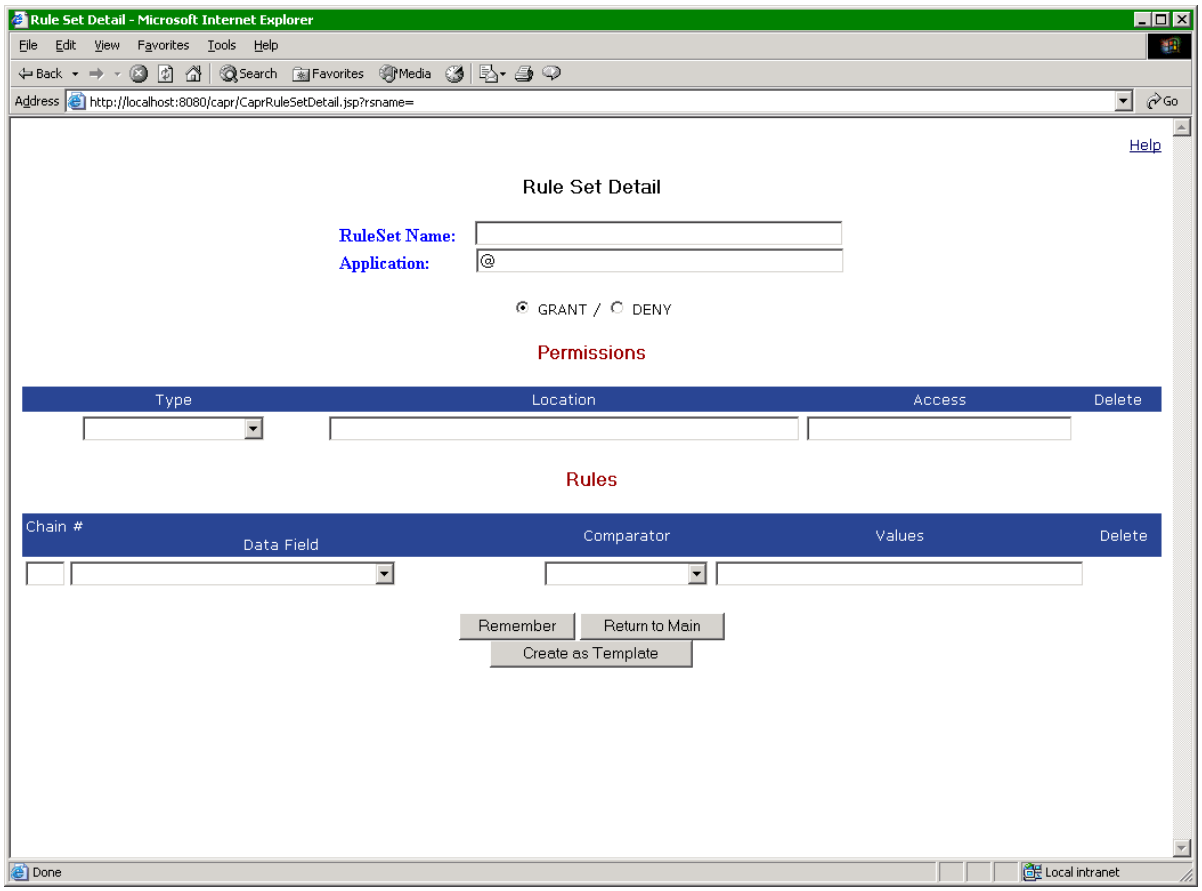

Figure 3-3. Rule Set Detail

This page allows the user to specify all of the attributes of a new RuleSet. A RuleSet is a conglomeration of Permission and Access Controls to restrict access to sensitive resources. For an individual to be either GRANTED or DENIED access to specified Permissions, all Rules must evaluate to true for a given certificate. Permission objects are used to specify what type of access is granted.

3. Add the attributes of the new RuleSet based on the descriptions provided below.

RuleSet Name

The name of the RuleSet. A user defined field used primarily to identify RuleSets for logging and modification purposes. This MUST BE UNIQUE, no duplicate names are allowed by the system, otherwise existing RuleSets will be overwritten.

Application

The application for which this RuleSet applies. Specified as application@host. If no host is specified the RuleSet is assumed to apply to all hosts on a given application. Wildcards are supported for both the application and host names.

Sense

Either GRANT or DENY, describing whether the client is granted or denied permission if the RuleSet evaluates to true.

Permission Detail Fields

Permission

The name of the Java Permission object. This object is a representation of the access type. For example if the administrator wishes to grant a specific individual access to a Url, they use an UrlPermission. The list of supported Permissions can be modified in the CAPR property file.

Location

The location this permission describes (i.e., c:\java\bin\ or http://www.yahoo.com). Depending on the type of Permission described above, different locations are appropriate and supported (i.e.,. for a UrlPermission a URL should be specified). For Url and File Permissions wildcards are supported. A '*' character can be used to specify all files within a given directory, while a '-' character is used to describe all files in the given directory as well as files in any subdirectory (i.e., c:\java\- or http://localhost/*).

Access

Unique values for each Permission type that describes the permitted actions on the location given above. For the common permissions the associated access values are listed below (note they may be used in any order and comma separated combinations of values are supported):

FilePermission - read, write, delete, execute

UrlPermission – read

SocketPermission - connect, accept, listen, resolve

ApplicationPermission - (any value)

AllPermission - (not applicable)

Rule Detail Fields

Datafield

This field is made up of two input areas, the chain number followed by the certificate field. The chain number is the first smaller of the two data input regions. This is only used when the user wishes to specify a rule concerning a certificate in the Certificate Authority (CA) Chain. The chain number specifies which certificate the rule applies to, starting with 0 as the user certificate, and 1 as the signer of that certificate. All rules without chain numbers are assumed to represent the user certificate. Chain numbers can only be specified for rules in which this second field begins with Subject.DistinguishedName. The second field is a drop down menu of all the fields within the certificate that are parsed.

Values

A comma-separated list of values. These values are compared to those obtained from the client certificate in the data field defined above. This comparison is done based on the Comparator (defined below), the result of which is the basis for granting or denying the permission defined in the Permissions section of this page.

Comparator

The operator to be applied in the comparison between DataField and Values. Most commonly this will be either EQUALS or NOTEQUALS. When a list of values is specified the operator will be applied to each of the values. Only one must hold for the RuleSet to evaluate to true. With the exception of the NOTEQUALS for which a not in list operation is used.

Remember Button

This button saves changes to the RuleSet.

Return to Main Menu Button

This button returns the user to the main CAPR menu.

Create as Template Button

This button allows the user to save the current Rule Set as a Template. After being redirected to the Rule Set Template page, the user has the option to export a template to the Rules Database thereby making it ready for implementation.

Example RuleSet Implementations

For example, an administrator wants to allow John Smith access to a web page located at http://www.fdle.gov/prisonrecords.html. He would create a new RuleSet with any name, the application being the web server which hosts that page, and the sense to GRANT. Set the Permission object to type = UrlPermission, location = http://www.fdle.gov./prisonrecords.html, access = read. And the Rule datafield = Subject.DistinguishedName.CommonName (no chain number need be specified), values = "John Smith" (quotes need not be entered), and comparator = INLIST.

As another example, the administrator wants to disallow everyone not in FDLE access to a file at c:\fdle\prisonrecords.doc. Again, create a RuleSet with any name, application = a name describing the group of files or directories to which the prisonrecords.doc belongs, sense = DENY. Set the Permission object type = FilePermission, location = c:\fdle\prisonrecords.doc, access = read, write. And the Rule datafield = Subject.DistinguishedName.CJNetOrganization, values = "FDLE", and comparator = NOTINLIST.

Editing a RuleSet

1. On the CAPR Main page, click on the name of the existing RuleSet in the table.
2. The Rule Set Detail screen displays.
3. Modify the properties for the RuleSet.
4. Click **Remember** to save the changes.
5. Click **Return to the Main Menu**.
6. On the CAPR Main page, click **Update RulesDB** to save the changes to the database.
7. If the CADES was running during this process it must be cycled. See the CADES Administrator Tool section of this document for instructions.

Deleting a RuleSet

1. On the CAPR Main page, mark the box in the Delete column of the RuleSet to be deleted.
2. Click **Update RulesDB** to delete the RuleSet from the database.

Test Certificate Extraction

This function allows the user to test the extraction of a Base-64 encoded certificate.

1. On the CAPR Main screen, click the Test Certificate Extraction link on the Other Tools menu.
2. The Certificate Test Extraction screen appears.
3. Paste the Base-64 encoding certificate including "BEGIN CERTIFICATE" and "END CERTIFICATE" definitions into the large text area.
4. After the certificate has been inserted properly, click the **TextExtract** button.

***Restrictions**: Certificates that are signed by untrusted Certificate Authorities will not extract properly. Additionally, self-signed certificates must also be listed in the trusted root store to perform extraction. To insert a certificate to the trusted root store, return to the main menu and 'Add Certificate Authority'.*

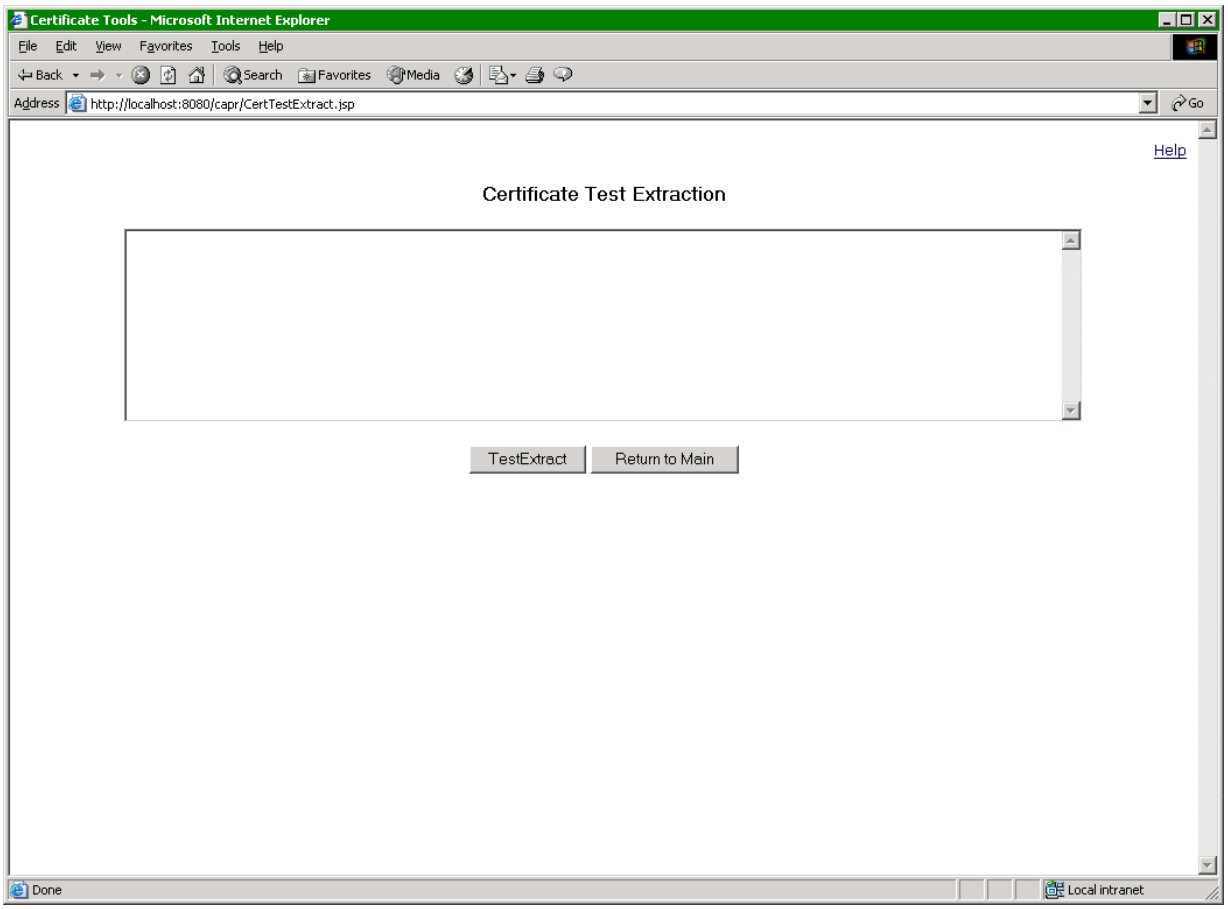

Figure 3-4. Certificate Test Extraction Screen

The return screen consists of two columns, Name & Value. Name is the field name of the extracted certificate value. This is the same field name as indicated in the Datafield section of the RuleSet Detail page (see configuration documentation to change names of extracted fields). Value is the actual value found in the certificate for the indicated field. Using similar notation to that found in the RuleSet Detail page chain numbers preceded field names where appropriate showing field values for Certificate Authorities as well. This gives a complete list of names and values available for RuleSet creation for a particular certificate.

Add Certificate Authority

This tool allows the user to add Certificate Authorities (CAs) to CBAC's trusted root store. Certificates will not be evaluated against the RuleSets if they are not signed by one of CBAC's trusted CAs. For chained CAs all signing certificates must be in the trusted store before signed certificates can be added (self signed root CAs should be added first).

1. On the CAPR Main page, click the Add Certificate Authority link on the Other Tools menu.
2. To add a CA, paste the Base-64 encoding of the Certificate into the indicated text area.
3. Enter a unique CA Name for the certificate authority. This name will identify the CA on the CA List.
4. Click the **Add CA** button. If the CA is successfully added its Distinguished Name information will be included in the list of trusted CAs.

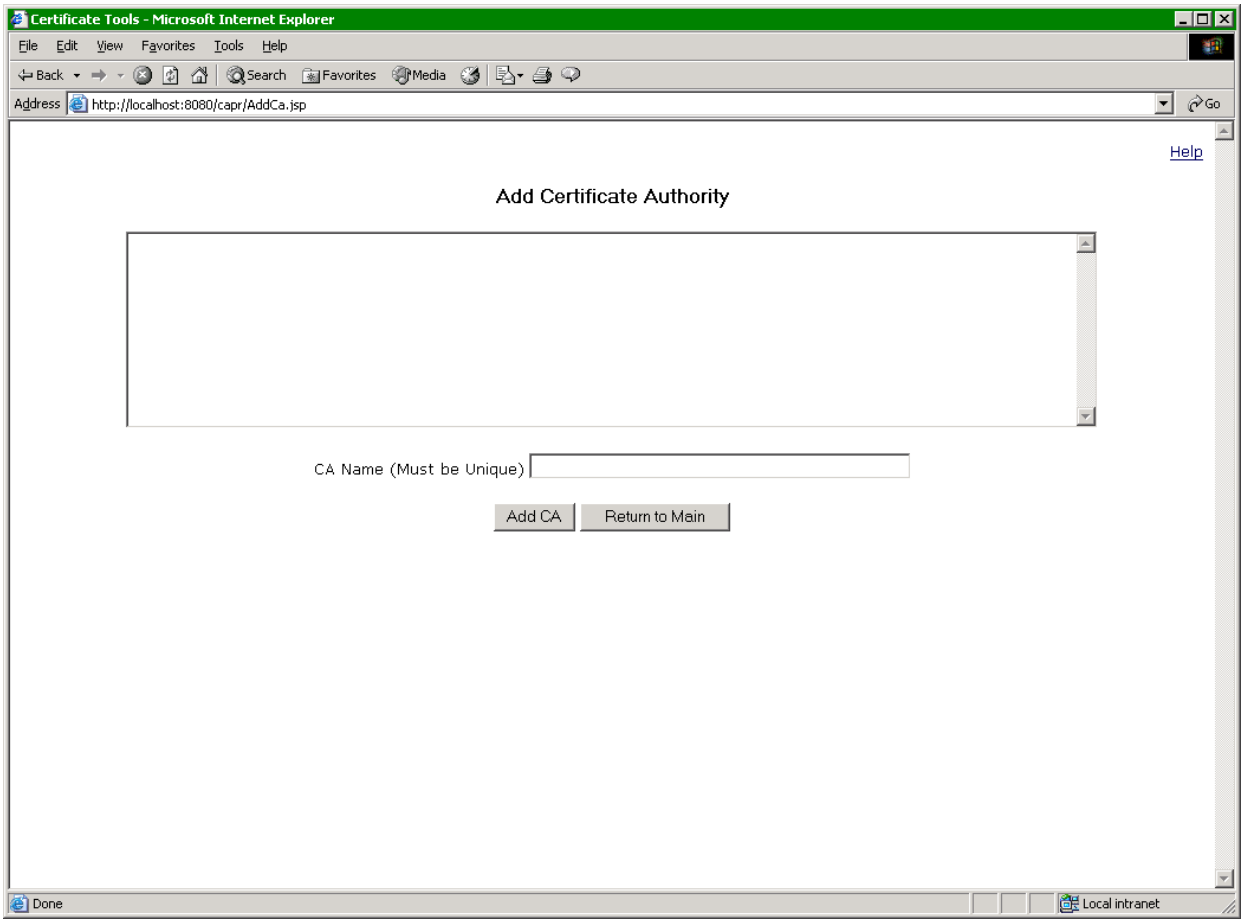

Figure 3-5. Add Certificate Authority Screen

List / Delete CAs

This function lists all of the Trusted Certificate Authorities (CA) within the CA Database, sorted by their Subject Distinguished Name fields. To delete a CA, mark the Delete check box corresponding to the CA to be deleted. Click Save to remove the CAs from the Rules Database.

Note: It is not necessary to also Update RulesDB on the Main Page to delete a CA from the list. To add a Certificate Authority please see the 'Add Certificate Authority' procedure.

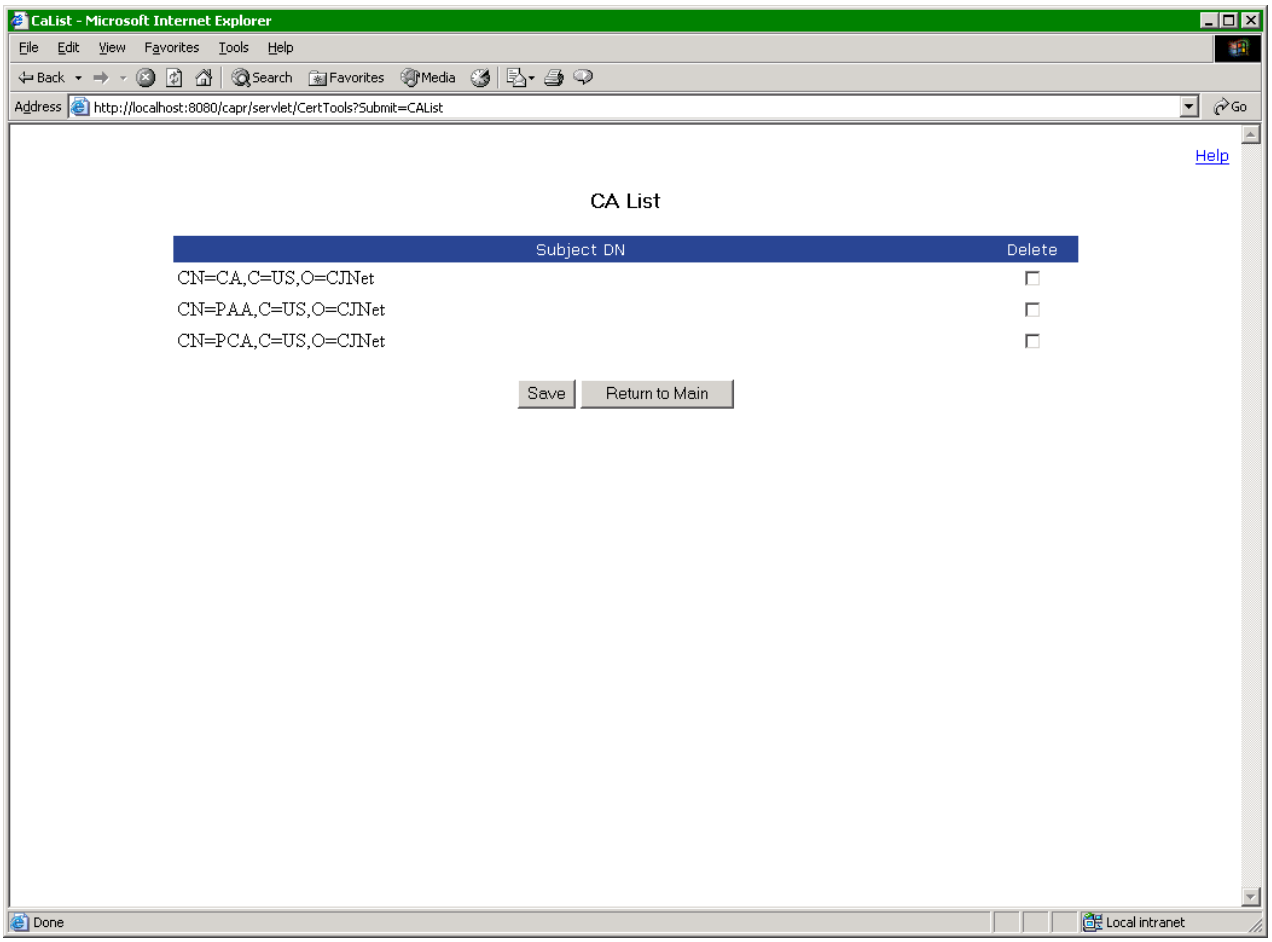

Figure 3-6. CA List Screen

Scan Rule Sets

This tool is used by administrators to verify that no rules exist that are not being used. The system permits the creation of Grant rules, which may never be checked if their permissions are implied by another Deny RuleSet. This system scans checks for any such rules and displays them in a chart.

Note: There are no guarantees that the listed RuleSets are actually masked. The system is unable to determine any hierarchy relating to the Rules. It simply evaluates application and permission implications when scanning.

The resulting page has two columns: Deny Name and Grant Name. Deny Name will list the name of the Deny Rule Set that may be masking a set of Grants. In an indented fashion the list of all of the Grant Rule Sets are listed in the right column. Each of these Names takes an administrator to the RuleSet Detail page allowing for the modification of RuleSet parameters.

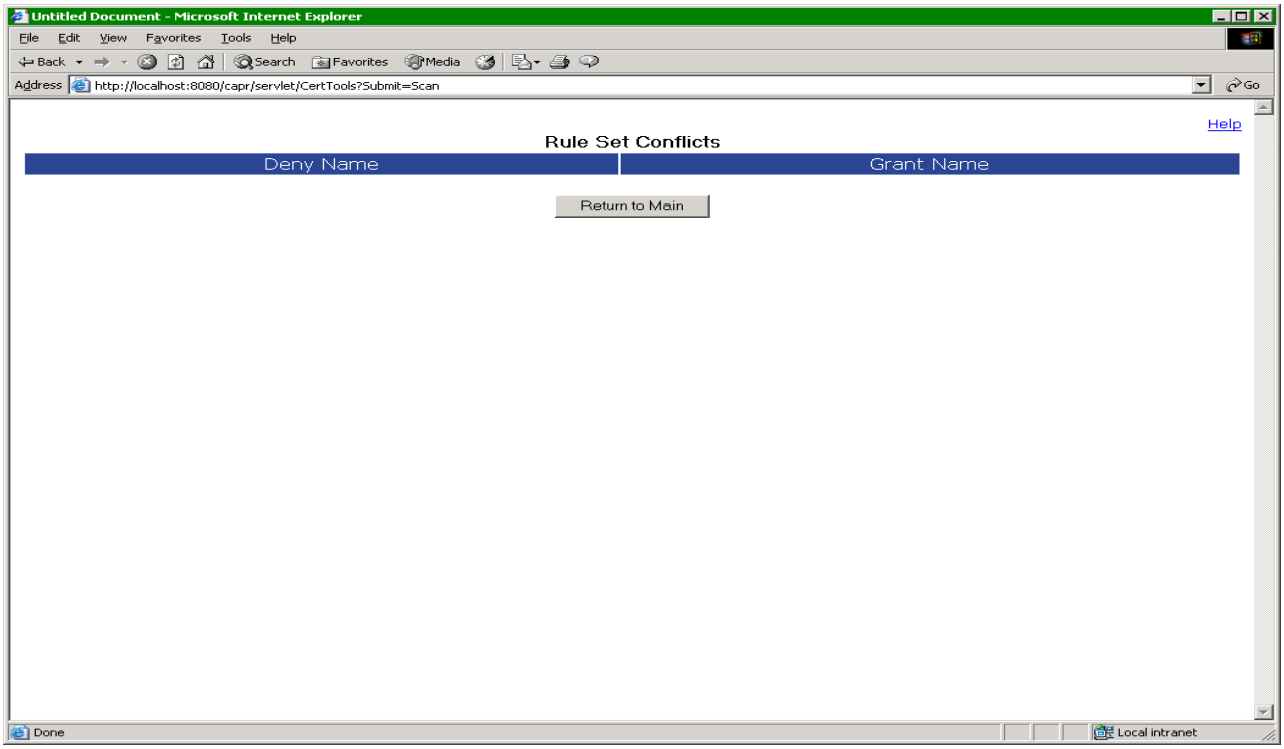

Figure 3-7. Rule Set Conflicts Screen

Rule Set Templates

This tools displays a list of Rule Set Templates, which can be used as a basis for other users to create their own Rule Sets. This feature is specifically designed for users who do not have much knowledge of Rule Sets and Certificates. This feature allows the user to create a basic outline for a Rule Set defining Rules as needed and save them as templates.

Users can export existing templates by selecting the export check box next to the appropriate RuleSetName and pressing the 'Export' button. Please Note: Only one template may be exported at a time. Exporting a template will take you to the RuleSet Detail page allowing a user to make modifications necessary to convert the template into a real Rule. Templates may also be deleted by selecting the list of templates using the delete checkboxes and pressing the Update button. All Templates contain the word TEMPLATE in their names. If this is removed from the name, the template will be deleted.

1. On the CAPR Main page, click **Add RuleSet**.
2. Set the name and any Rules and Permissions that apply
3. Save the Rule Set as a template by clicking the **Create As Template** button.

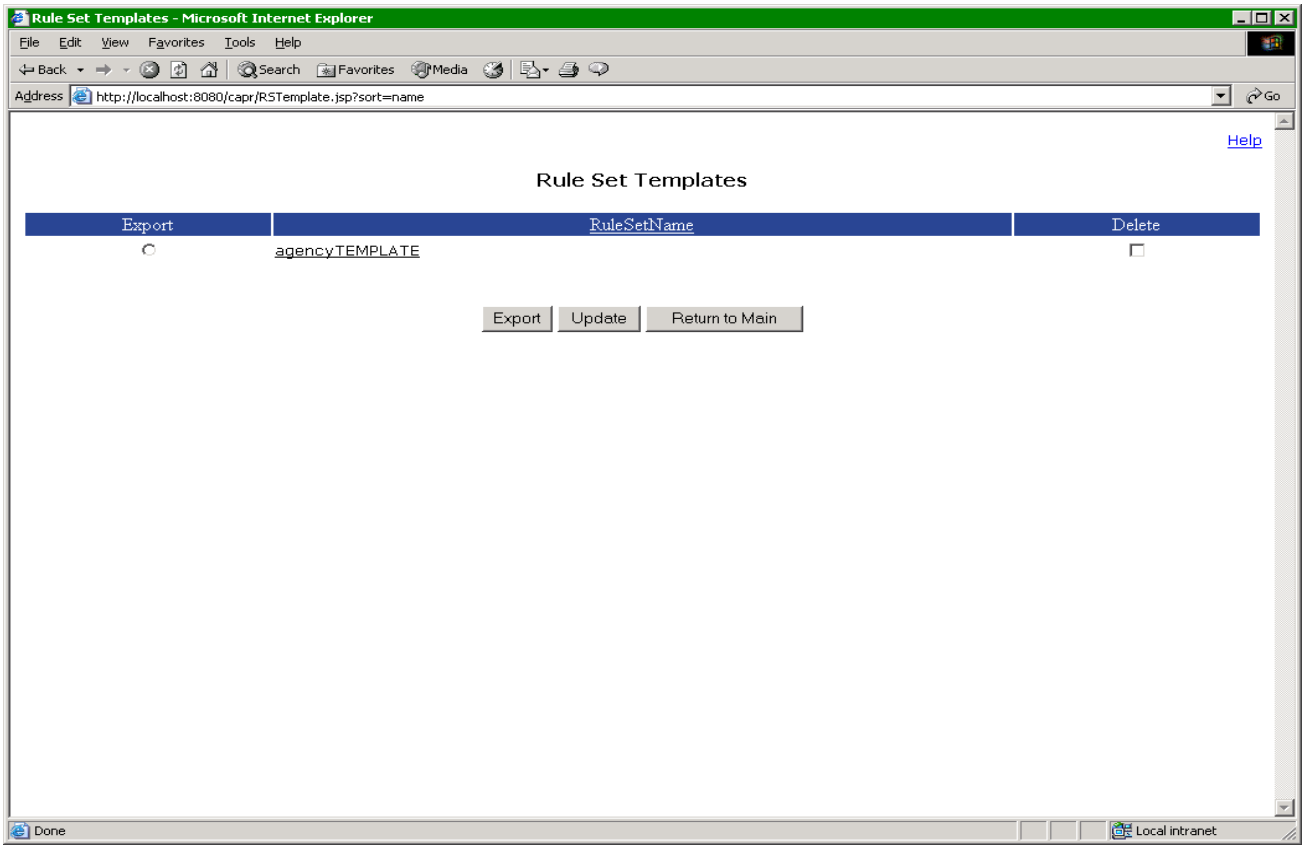

Figure 3-8. Rule Set Templates Screen

CADES Administrative Tool

This tool allows an administrator to force specified Query Servers to reload rules from the Rules Database. All of the information concerning the remote CADES systems is obtained from an ldap servers which is updated with accurate information in real time. By selecting from the check box on the right and then pressing the Cycle CADES, button an administrator cycles the remote servers in turn forcing them to re-load modified rule sets.

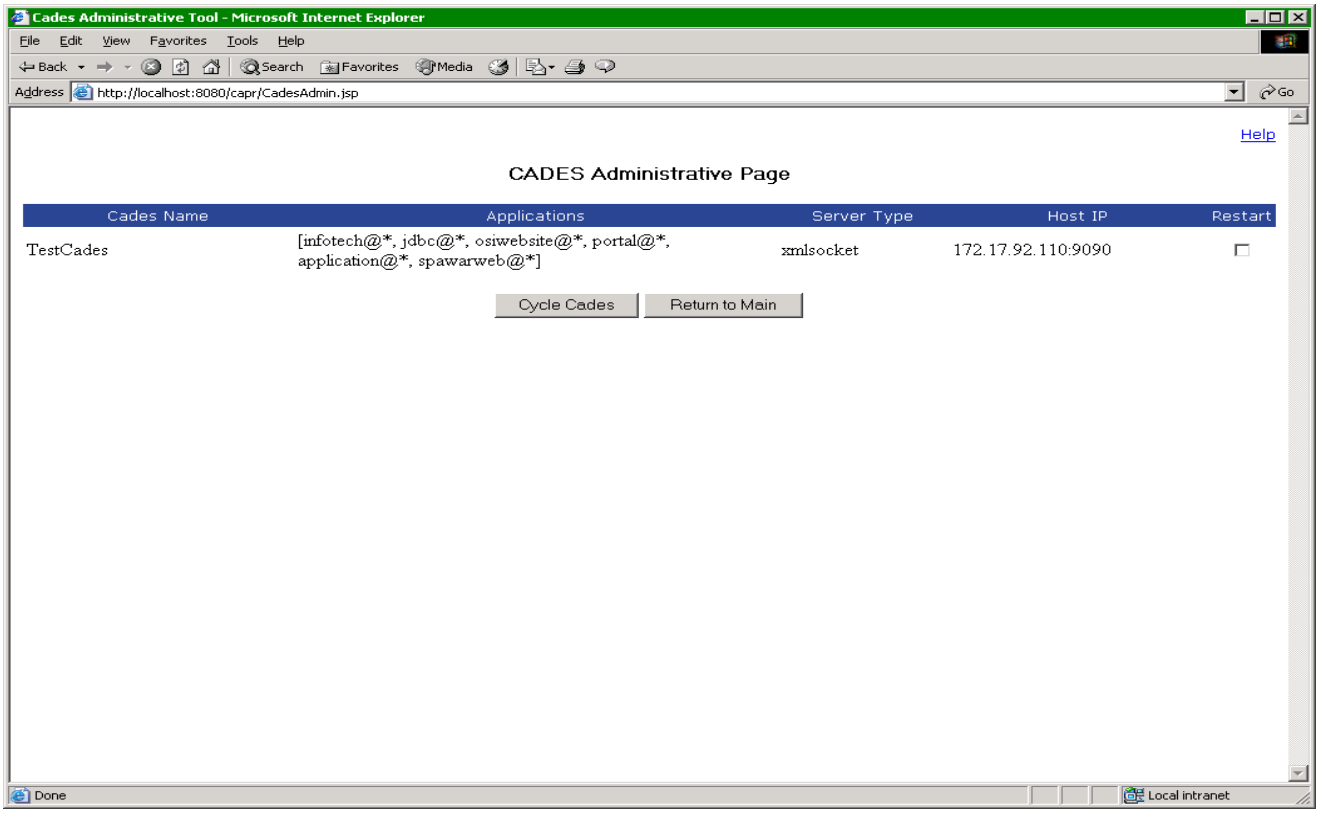

Figure 3-9. CADES Administrative Tool Page

Cycle the CADES

1. Go to the CADES Admin Tool page
2. Go the the Restart column and check the box of the appropriated CADES to cycle.
3. Click the Cycle Cades button and the CADES will be cycled.

Cades Name

The user specified name of each remote running Cades server, obtained from the pertinent Cades property file

Applications

A comma separated list of the applications which this Cades supports

Host

The fully qualified host name of the Cades Server (i.e.,rmi://127.0.0.1:/cades [rmi] or 176.5.4.3:9090 [socket])

Server Type

The network transport protocol used by the specified Cades server (Supported values currently include: socket, rmi, and corba)

Appendix A Operator Messages

CADES

System.out

"All security providers loaded"

Meaning Java Security Provider was loaded properly

"Cades RMI Server Registered [CADES Name]"

CADES properly bound to RMI Registry

"Error loading provider [provider name] [error]"

Error occurred while loading the specified provider

"Error registering CADES RMI [error]"

Error while binding CADES to RMI Registry

Log Messages

"Certificate Revocation List Loaded"

Certification Revocation List loaded properly

"Cades Started Without CRL"

No CRL was specified on startup.

"Error Loading CRL [CRL Location]"

Failed while attempting to load Revocation List

“Application's Rules Loaded: \n [List of Applications]”

List of applications whose rules are loaded

“This Certificate has been revoked”

Certificate was revoked by CRL

“No cert serial number”

Certificate is lacking a proper Serial Number

“Permission denied”

Access denied

“Permission granted? [true/false]”

Whether or not permission granted

“RuleSet Evaluated to True: [RuleSet Name]”

The name of the RuleSet, which evaluated to true

“Sense: [GRANT\DENY]”

The sense of the above RuleSet

System Errors

All system errors are dumped to the Log File.

CAPR

All CAPR Messages are output directly to the web interface and are designed to be self-explanatory.

All CAPR System Errors are presented to users on an Error page with instructions as to whom to contact concerning the unexpected system behavior.