

CSM 4.1 GAARDS MIGRATION MODULE

Version 0.5 – Technical Guide



**NATIONAL[®]
CANCER
INSTITUTE**

Center for Biomedical Informatics
and Information Technology

This is a U.S. Government work.

November 14, 2008

Revision History

The most current version of this document is located on the CSM website:
<http://ncicb.nci.nih.gov/core/CSM>.

Revision History

<i>Revision Date</i>	<i>Author</i>	<i>Summary of Changes</i>
10/31/2008	Vijay Parmar	Initial Table of Contents
11/05/2008	Vijay Parmar	Added new chapters
11/10/2008	Charles Griffin	Review of initial draft
11/12/2008	Bronwyn Gagne	Doc converted to current CBIIT template, and edited as necessary.
11/14/2008	Vijay Parmar, Bronwyn Gagne	Final review and Release of updated 4.1 guide.

Table of Contents

About This Guide	1
Purpose	1
Scope	1
Topics Covered	1
Related Documentation	2
Text Conventions Used	2
Credits and Resources	3
Chapter 1 CGMM Overview	5
CGMM Architecture	5
CGMM Solutions	6
CGMM Process Flow	7
CGMM Components	7
Security Concepts	8
Minimum System Requirements	9
Chapter 2 Using the CGMM API	11
Workflow	11
CGMM API Services	12
CGMMManager	12
Integrating with the CGMM API	16
Importing the CGMM Authentication API	16
Obtaining the CGMMManager	17
Authenticating Users	17
Migrating Users	17
Integrating Auto Start SyncGTS servlet	18
Configurations for CGMM API	18
Chapter 3 Using the CGMM Tool	21
Workflows	21
Workflow Scenario 1: User Logs In with CSM Account	22
Workflow Scenario 2: User Logs In with caGrid Account	28
Configuring the CGMM Tool	32
Chapter 4 CGMM Installation and Deployment	33
Release Contents	34
Installation Pre-Requisites	34
Refactoring Host Application	35
caGrid Security Infrastructure	35
Identify Configuration Parameters for CGMM	36
Deployment Checklist	36
Deployment Steps	37
Appendix A CGMM Properties XSD File	41
Appendix B Sample CGMM Properties File	45
Appendix C Sample Sync Description File	47
Appendix D Sample Install of CGMM with Reference Implementation	49
Glossary	53

Index 55

About This Guide

This preface introduces you to the *CSM GARRDS Migration Module (CGMM) Technical Guide*.

Topics in this section include:

- [Purpose](#) on this page
- [Scope](#) on this page
- [Topics Covered](#) on page 1
- [Related Documentation](#) on page 2
- [Text Conventions Used](#) on page 2
- [Credits and Resources](#) on page 3

Purpose

This guide provides all the information application developers need to successfully use the CSM GAARDS Migration Module (CGMM). The CGMM was chartered to provide a comprehensive solution to migrate existing web applications from CSM based authentication to GAARDS based authentication. caGrid is the underlying service oriented infrastructure that supports caBIG[®]. The Grid Authentication and Authorization with Reliably Distributed Services (GAARDS) provides services and tools for the administration and enforcement of security policy in an enterprise Grid. GAARDS was developed on top of the Globus Toolkit and extends the Grid Security Infrastructure (GSI) to provide enterprise services and administrative.

Scope

This document covers the CGMM API and CGMM Web application. It covers the workflows/scenarios handled by the CGMM. This document also briefly addresses the host application enhancements that are required to adopt the CGMM based authentication and migration features.

The caGrid information pertaining to the CGMM is provided, however the caGrid, GAARDS, SyncGTS, Dorian etc details are out of scope for this document. For more information about caGrid and related technologies refer caGrid Wiki located at: <http://www.cagrid.org/mwiki/index.php?title=CaGrid>.

Topics Covered

This brief overview explains what you will find in each section of this guide.

- [Chapter 1, CGMM Overview](#) provides an overview of CGMM and its capabilities.
- [Chapter 2, Using the CGMM API](#) provides the necessary information and workflow for a developer to successfully integrate the CGMM API into their application.

- [Chapter 3, Using the CGMM Tool](#) provides a workflow and details for using the CGMM Tool for authentication, migration, and/or new caGrid user creation.
- [Chapter 4, CGMM Installation and Deployment](#) provides the information and steps necessary to install and deploy the CGMM Tool with a working installation of a host application.
- [Appendix A, CGMM Properties XSD File](#) provides a sample CGMM properties XSD file.
- [Appendix B, Sample CGMM Properties File](#) provides a sample CGMM properties configuration file.
- [Appendix C, Sample Sync Description File](#) provides a sample Sync Description configuration file.
- [Appendix D, Sample Install of CGMM with Reference Implementation](#) provides the steps necessary to install the reference implementation `cgmmHostWeb` web application along with the `cgmmweb` web application.

The Glossary, located behind the appendices, is provided to clarify abbreviations and terms used in this document.

Related Documentation

More information can be found in the following related CSM documents:

- Common Security Module (CSM) v4.1 Technical Guide
- CSM GAARDS User Migration Design Document.

These and other documents can be found on the CSM website:

http://ncicb.nci.nih.gov/NCICB/infrastructure/cacore_overview/csm

Additional information and FAQ regarding the CGMM are available from the CSM Wiki page located at: <https://wiki.nci.nih.gov/x/4wBB>.

Text Conventions Used

This section explains conventions used in this guide. The various typefaces represent interface components, keyboard shortcuts, toolbar buttons, dialog box options, and text that you type.

Convention	Description	Example
Bold	Highlights names of option buttons, check boxes, drop-down menus, menu commands, command buttons, or icons.	Click Search .
URL	Indicates a Web address.	http://domain.com
text in SMALL CAPS	Indicates a keyboard shortcut.	Press ENTER.
text in SMALL CAPS + text in SMALL CAPS	Indicates keys that are pressed simultaneously.	Press SHIFT + CTRL.

Convention	Description	Example
<i>Italics</i>	Highlights references to other documents, sections, figures, and tables.	See <i>Figure 4.5</i> .
<i>Italic boldface monospace type</i>	Represents text that you type.	In the New Subset text box, enter <i>Proprietary Proteins</i> .
Note:	Highlights information of particular importance.	Note: This concept is used throughout this document.
{ }	Surrounds replaceable items.	Replace {last name, first name} with the Principal Investigator's name.

Credits and Resources

caCORE CSM Development and Management Teams		
CSM Development Team	Documentation	Program Management
Vijay Parmar ¹	Vijay Parmar ¹	Dave Hau ³
Aynur Abdurazik ²	Charles Griffin ¹	Charles Griffin ¹
	Bronwyn Gagne ⁴	
¹ Ekagra Software Technologies	² Science Applications International Corp. (SAIC)	³ National Cancer Institute Center for Biomedical Informatics and Information Technology
⁴ Lockheed Martin		

CSM Resources	
Name	URL
Mailing List	security-csm-user@gforge.nci.nih.gov
Mailing List Archive	http://gforge.nci.nih.gov/pipermail/security-csm-user
GForge Project Home	http://gforge.nci.nih.gov/projects/security
CSM Support Tracker	http://gforge.nci.nih.gov/tracker/?atid=131&group_id=12&func=browse

Contacts and Support	
NCICB Application Support	http://ncicb.nci.nih.gov/NCICB/support Telephone: 301-451-4384 Toll free: 888-478-4423

Submitting a Support Issue

A GForge *Support* tracker group, which is actively monitored by CSM developers, has been created to track any support requests. If you believe there is a bug/issue in the CSM software itself, or have a technical issue that cannot be resolved by contacting the [NCICB Application Support](#) group, please submit a new support tracker using the following link:

https://qforge.nci.nih.gov/tracker/?atid=131&group_id=12&func=browse.

Make sure to review any existing support request trackers prior to submitting a new one in order to help avoid duplicate submissions.

Release Schedule

This guide was created to correspond with the 4.1 version of caCORE CSM and the CSM GAARDS Migration Module, which was released in November 2008 by the NCI Center for Biomedical Informatics and Information Technology (CBIIT), formerly the National Cancer Institute Center for Bioinformatics (NCICB).

Chapter 1 CGMM Overview

The chapter provides an overview of the architecture, and discussions of the components involved in the CSM GAARDS Migration Module (CGMM), security concepts, and minimum system requirements. Topics in this chapter include:

- [CGMM Architecture](#) on this page.
- [CGMM Components](#) on page 7.
- [Security Concepts](#) on page 8.
- [Minimum System Requirements](#) on page 9.

CGMM Architecture

The CGMM provides a two-tiered solution for existing web applications, namely to:

1. Migrate existing CSM accounts to caGrid accounts,
2. Act as the authentication 'module' for the host application.

By doing so, the existing web applications gradually avail a single set of credentials (caGrid credentials) for authentication purpose.

CGMM has been created to address the following business/policy requirements:

- Avoid duplication of accounts for existing and new users. The application needs to provide a single set of credentials to access various application components.
- Ability to use GAARDS based authentication.
- Provisioning of new users with Grid identities.
- To use caBIG approved identity providers, thus allowing federation of identities.
- Provide a configurable "Look and Feel"
- Provide configurable caGrid identity providers for authentication.

As shown in Figure 1-1 below, the CGMM architecture allows existing host applications to integrate with CGMM and sort of "off-load" their authentication functionality to CGMM. CGMM is expected to intercept and migrate CSM (local) accounts, and enforce the use of caGrid accounts offered by various Identity providers in caBIG.

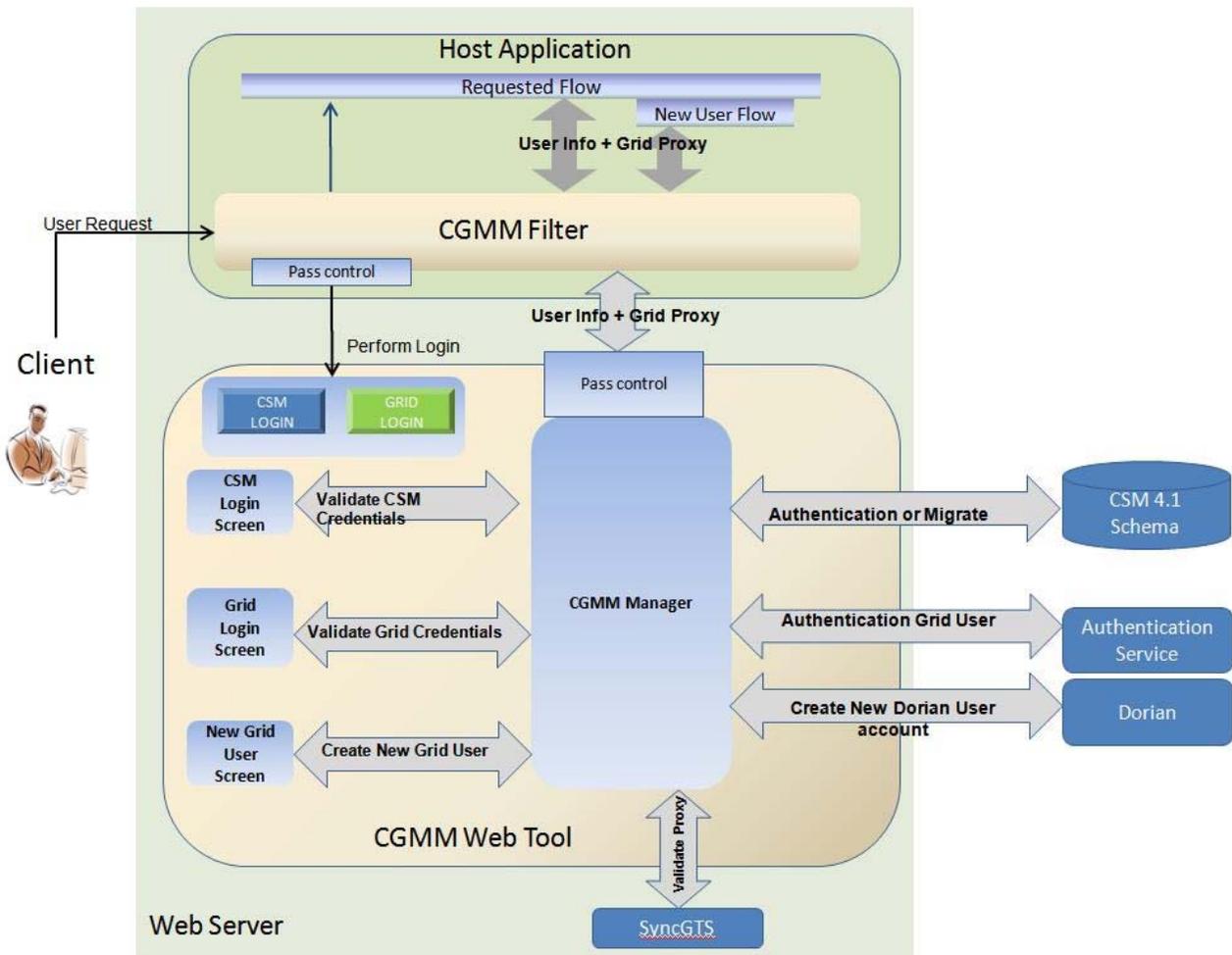


Figure 1-1 CGMM Architecture

The above diagram demonstrates the overall architecture of CGMM, the components involved, and their interactions at a high level. As shown, CGMM is a web application that is hosted on the same application server as the Host web application. The Host application uses a migration filter, *CGMMMigrationFilter*, provided by the CGMM to forward all un-authenticated user requests. The GAARDS components used are *Authentication Service*, *Dorian Service*, and *SyncGTS*.

CGMM Solutions

The CGMM provides the following solutions for the host application:

Authentication – CGMM validates and verifies a user’s CSM (local) credentials to initiate migration, and validates and verifies a user’s caGrid Login ID and password against an Authentication Service. Once an already migrated user is authenticated, the CGMM passes the control to the host application by providing the user’s information and Grid Proxy.

Migration – CGMM migrates or transforms a CSM user to a caGrid user. The migration involves updating the CSM account (Login ID) information with the caGrid account (Login ID) in the CSM schema of the host application.

New caGrid User Creation – CGMM creates a new caGrid (Dorian) account for a new or existing User. Once the user has a caGrid account, the CGMM can migrate the user for the host application.

Configurable CGMM Tool – CGMM allows for the enabling or disabling of the New caGrid User creation feature of the CGMM Tool. CGMM also allows for the configuration of other information, such as host application information and Authentication Service and Dorian Service information.

CGMM API – The CGMM API allows programmatic access and integration of the CGMM features.

CGMM Process Flow

The overall flow for CGMM is as follows:

1. A user accesses Host applications secured page.
2. An Http filter intercepts the user's request. The filter checks the session for user information attributes to verify if a user is logged in or not. If user is not logged in then the filter routes the user to CGMM.
3. CGMM module authenticates the user, migrates the user, and obtains Grid proxy.
4. CGMM passes control back to the Host application and provides the Grid proxy and user information attributes. If the authenticated user did not have CSM credentials, then the control is passed to the new user creation workflow of the Host application. Otherwise the control is passed back to the user's home page.
5. The filter intercepts the request and verifies user is logged in. Filter gets the Grid proxy and user information attributes. The filter sets this information in Session.
6. The filter gives up control to forward the request to the host application. The Host application uses the user information from session for authorization.

CGMM Components

The following are the minimum set of components involved in the CGMM Framework. This section describes the components shown in the CGMM Architecture diagram above (Figure 1-1).

CGMM Filter (in the host application)

A new HTTP filter (provided as part of the CGMM) is configured by the host application to intercept and forward the user requests to the CGMM, to either migrate the user account or to log the user into the Host application. Depending on whether the user is an existing application user or not, control is passed back to either the login workflow or the new user creation workflow respectively.

CGMM Tool

The CGMM Tool is provided to assist in the migration of local CSM accounts to caGrid accounts. Performing this migration allows GAARDS-based authentication to the host application via single set of credentials. The CGMM Tool is a separate web

application that resides in the same container as the Host web application. CGMM also provides the Servlet Filter that gets placed in front of the host application, intercepting and routing each user request for login or migration purpose. A detailed workflow of the migration module and the considered scenarios are provided in [Chapter 3, Using the CGMM Tool](#) on page 21.

Authentication Service

The IdPs registered on NCICB Production Grid are used as the Identity Provider to validate user's credentials. They authenticate the user and provide a SAML token.

Dorian

The NCICB Production Dorian is used as a Federation Service to generate the user's grid identity. This Dorian instance also hosts all the users migrated from individual local host application instances that are not associated with any other Identity Providers (IdPs).

SyncGTS

SyncGTS is installed in CGMM for the host application. The SyncGTS daemon keeps the host application in sync with the Grid Trust Fabric, and updates the CRL's accordingly. Once the CGMM obtains Grid proxy from Dorian, it validates the proxy against the GTS to make sure the certificate is still valid and has not been revoked.

Security Concepts

In order to successfully integrate CGMM with an existing host application, it is important to understand the definitions for components, systems, and services involved as defined in the table below. Application Developers should understand these concepts and begin to understand how they apply to their particular application.

Concept	Definition
Host Application	The web application integrating with the CGMM Tool. The host web implements the CGMM Filter, and all unsecured access to the web application is forwarded to the CGMM Tool.
CGMM API	The CGMM API provides a CGMMManager interface to programmatically access all features of the CGMM Tool such as authentication of CSM users, authentication of caGrid users, creation of new caGrid accounts, etc.
CGMM Tool	The CGMM Tool is a web application that is deployed in the same container as the host application. The CGMM Tool does all the authentication, migration, and new Grid user creation activities for the host application.
CSM User	Any user that has been provisioned in the CSM 4.1 Schema of the Host application. This user indicates the existence of the Host Application User with appropriate User Provisioning (assignment/association of Groups/ Protection Element/ Protection Groups to Role/Privilege). The user may or may not have a caGrid account or caGrid identity.

Concept	Definition
caGrid User	Any user that has already created an account or registered to caGrid. The registration provides the login credentials for the user. Once a user has registered with caGrid and obtained an account, that user can be authenticated using the valid credentials via the GAARDS security framework or via Authentication Service or Dorian Service.
Migration of CSM Account to Grid Account	The act of updating the CSM Login Name, in the CSM 4.1 Schema's CSM_USER table, with the caGrid User identity and marking the particular user as migrated is known as migration of CSM account to caGrid account. An already migrated user can be authenticated using caGrid Login ID and password.

Table 1-1 Security concept definitions

Minimum System Requirements

The software listed in the table below is required and is not included with CGMM. The product name, version, description, and URL hyperlinks are provided.

Software	Description	Version	URL
JDK	The J2SE Software Development Kit (SDK) supports creating J2SE applications.	1.5.0_11 or higher	http://java.sun.com/j2se/1.5.0/download.html
Oracle	Database Server (Only one is required)	9i	http://www.oracle.com/technology/products/oracle9i/index.html
MySQL		5.0.27	http://dev.mysql.com/downloads/mysql/5.0.html
JBoss	Application Server (Only one is required)	4.0.5	http://labs.jboss.com/jbossas/downloads
Tomcat		5.5.20	http://tomcat.apache.org/download-55.cgi
Ant	Build Tool	1.6.5 or higher	http://ant.apache.org/bindownload.cgi
caGrid	caGrid software	1.2	https://cabig.nci.nih.gov/workspaces/Architecture/caGrid/
Globus	Globus Toolkit	4.0.3	Globus WS-Core with WS-Enum Support

Table 1-2 Minimum Software Requirements

Chapter 2 Using the CGMM API

The CGMM features are available as API's. The CGMM API primarily consists of the CGMMManager interface. The CGMM API was created for host applications that wish to incorporate the CGMM features in their code base. Integration of CGMM API is not a requirement and is completely up to the development team to either adopt the CGMM tool (least changes to host application way) or integrate the CGMM functionality via API (more changes to host application authentication and migration logic).

Alternatively, the CGMM API can be used in different ways to suit the host applications requirement or also in standard java applications that can be run via automated scripts.

Topics in this chapter include:

- [Workflow](#) on this page.
- [CGMM API Services](#) on page 12.
- [Integrating with the CGMM API](#) on page 16.
- [Configurations for CGMM API](#) on page 18.

Workflow

This workflow section outlines the basic steps, both strategic and technical, for successful CGMM API integration.

1. Read the CSM GAARDS Migration Module Guide (this document). It provides an overview, workflow, and specific deployment and integration steps and CGMM Tool user guide.
2. Decide which services you would like to integrate with your host application. If the application should authenticate CSM (local) users against an LDAP or other directory, select CSM Authentication. If the application should authenticate caGrid users against Authentication Service(s), select caGrid Authentication. If the host application would like to create new caGrid users, select new caGrid user creation feature. The migration feature should be used to migrate the CSM (local) user ID to the caGrid ID of the user. See the [CGMM API Services](#) section more details.
3. Add the StartSyncGTSServlet servlet to your host web application. See [Integrating Auto Start SyncGTS servlet](#) on page 18 for more details.
4. Integrate the application code using the integration as shown in the following sections
5. Test and refine CGMM integration with your application. Confirm that your CGMM API integration meets requirements.

CGMM API Services

The CGMM API's consist primarily of the following features: Authentication, Migration, new caGrid User creation, and synching with the caGrid Trust Fabric.

CGMMManager

The CGMM Manager is an interface that provides the functionality described in Table 2-1 below. This functionality is implemented by the *CGMMManagerImpl* class, available in the CGMM APIs, and includes the following:

- caGrid User Authentication and CSM Authentication.
- Migration of CSM Account to caGrid Account.
- New caGrid User Creation.
- Miscellaneous tasks, including:
 - get CSM User details
 - get caGrid User Attributes and Attribute Map
 - get Authentication Service URL Map.

The following table lists and describes all of the CGMMManager API methods that perform these tasks:

Class/Method	Description
public interface CGMMManager	<p>This CGMM Manager provides all the CSM GAARDS user migration related services offered by Common Security Module.</p> <p>This interface defines the contract for any class that wants to act as <i>CGMMManager</i>. It defines the methods required for authenticating CSM users, authenticating users with caGrid based accounts, and creating accounts on the configured Dorian.</p> <p>The <i>CGMMManager</i> is implemented by <i>CGMMManagerImpl</i>. <i>CGMMManager</i> can be configured using the <code>cgmm-properties.xml</code> configuration file.</p>

Class/Method	Description
<p>public boolean performCSMLogin(String userIDCSM, String password) throws CGMMInputException, CGMMConfigurationException, CGMMCSMAuthenticationException;</p>	<p>Authenticates user against the configured CSM credential provider. The CSM credential provider configuration can be done via CGMM configuration file.</p> <p>Parameters:</p> <p>userIDCSM The CSM User Login ID of the User. password The Password of the CSM User.</p> <p>Returns:</p> <p>true if login is successful.</p> <p>Throws:</p> <p><i>CGMMCSMAuthenticationException</i> is thrown when the credentials are invalid or other errors occur during validation.</p> <p><i>CGMMConfigurationException</i> is thrown when there is a CGMM configuration exception.</p> <p><i>CGMMInputException</i> is thrown when there is an error in specifying User Id/password.</p>
<p>public CGMMUser getUserDetails(String loginID) throws CGMMInputException, CGMMConfigurationException, CGMMCSMUserException ;</p>	<p>Updates the CGMMUser object with CSM User Details. Retrieves CSM user information from CSM schema using the CSM API's AuthorizationManager and populates the CGMMUser.</p> <p>Parameters:</p> <p>loginID The Login ID of the User available in CSM. This ID can be a caGrid ID or CSM Local User ID.</p> <p>Returns:</p> <p>CGMMUser</p> <p>Throws:</p> <p><i>CGMMCSMUserException</i> is thrown when there is an error obtaining the CSM User from the CSM schema.</p> <p><i>CGMMConfigurationException</i> is thrown when there is a CGMM configuration exception.</p> <p><i>CGMMInputException</i> is thrown when there is an error in specifying User Id/password.</p>

Class/Method	Description
<p>public boolean isUserMigrated(String userIDCSM) throws CGMMInputException, CGMMConfigurationException, CGMMMigrationException ;</p>	<p>Checks if the user is migrated or not. If the user is migrated then the Grid ID of the user is available in the CSM schema and the user is marked as migrated. If the user is not migrated, the CSM ID of the user is available in the CSM schema and hence the user is not marked as migrated.</p> <p>Parameters: userIDCSM The CSM User Login ID of the User.</p> <p>Returns: false if the user is not migrated.</p> <p>Throws: CGMMMigrationException is thrown when there is an error in migrating a CSM User to caGrid User. CGMMConfigurationException is thrown when there is a CGMM configuration exception. CGMMInputException is thrown when there is an error in specifying User Id/password.</p>
<p>public boolean migrateCSMUserIDToGridID(String userIDCSM, String userIDGrid) throws CGMMMigrationException, CGMMConfigurationException ;</p>	<p>Updates the users CSM ID with the user's Grid ID and also marks the user as migrated in the CSM Schema.</p> <p>Parameters: userIDCSM The CSM User Login ID of the User. userIDGrid The login ID for users caGrid account.</p> <p>Returns: false if migration failure.</p> <p>Throws: CGMMConfigurationException is thrown when there is a CGMM configuration exception. CGMMMigrationException is thrown when there is an error in migrating a CSM User to caGrid User.</p>

Class/Method	Description
<p>public GlobusCredential performGridLogin(String loginIDGrid, String password, String authenticationServiceURL) throws CGMMInputException, CGMMConfigurationException, CGMMGridDorianException, CGMMGridAuthenticationServiceExc eption, CGMMAuthenticationURLExeption ;</p>	<p>Authenticates the Grid credentials of the user against the provided Authentication Service URL.</p> <p>Parameters:</p> <p>loginIDGrid The login ID for users caGrid account. password The password for user caGrid account. authenticationServiceURL The URL for authentication service.</p> <p>Returns: GlobusCredential</p> <p>Throws: <i>CGMMGridAuthenticationServiceException</i> is thrown when there is an exception in caGrid's Authentication Service. <i>CGMMGridDorianException</i> is thrown when there is a Dorian exception. <i>CGMMConfigurationException</i> is thrown when there is a CGMM configuration exception. <i>CGMMInputException</i> is thrown when there is an error in specifying User Id/password. <i>CGMMAuthenticationURLExeption</i> is thrown when there is an Authentication Service URL specification exception.</p>
<p>public String createDorianAccount(CGMMUser cgmmUser, String dorianURL) throws CGMMAuthenticationURLExeption, CGMMGridDorianException, CGMMGridDorianUserPropertiesExc eption;</p>	<p>Creates a caGrid (Dorian) account.</p> <p>Parameters:</p> <p>cgmmUser The CGMMUser object populated with required fields for Dorian account creation. dorianURL The URL for Dorian Service</p> <p>Returns: Confirmation Message with the status of the Dorian account creation.</p> <p>Throws: <i>CGMMGridDorianUserPropertiesException</i> is thrown when there is an error in specifying Dorian User properties. <i>CGMMGridDorianException</i> is thrown when there is a Dorian exception. <i>CGMMAuthenticationURLExeption</i> is thrown when there is an Authentication Service URL specification exception.</p>
<p>public SortedMap getAuthenticationServiceURLMap() throws CGMMConfigurationException;</p>	<p>Provides the SortedMap of Authentication Service URLs.</p> <p>Returns: SortedMap of Authentication Service URLs. The Key is the Authentication Service Name and the value is Authentication Service URL</p> <p>Throws: <i>CGMMConfigurationException</i> is thrown when there is a CGMM configuration exception.</p>

Class/Method	Description
<pre>public HashMap<String, String> getUserAttributesMap(String loginIDGrid, String password, String authenticationServiceURL) throws CGMMInputException, CGMMConfigurationException, CGMMGridDorianException, CGMMGridAuthenticationServiceExc eption, CGMMAuthenticationURLException;</pre>	<p>Returns User Attributes Map based on the authenticated user.</p> <p>Parameters:</p> <ul style="list-style-type: none"> loginIDGrid The login ID for users Grid account. password The password for user Grid account. authenticationServiceURL The URL for authentication service. <p>Returns:</p> <ul style="list-style-type: none"> userAttributeMap containing the Users Attributes such as First Name, Last Name, and Email Id. <p>Throws:</p> <ul style="list-style-type: none"> <i>CGMMGridAuthenticationServiceException</i> is thrown when there is an exception in caGrid's Authentication Service. <i>CGMMInputException</i> is thrown when there is an error in the input provided. <i>CGMMConfigurationException</i> is thrown when there is a CGMM configuration exception. <i>CGMMGridDorianException</i> is thrown when there is an exception in caGrid's Dorian. <i>CGMMGridAuthenticationServiceException</i> is thrown when there is an exception in caGrid's Authentication Service. <i>CGMMAuthenticationURLException</i> is thrown when there is an Authentication Service URL specification exception.

Table 2-1 CGMM API - CGMM Manager

Integrating with the CGMM API

The CGMM API provides a CGMMManager for user authentication for CSM, user authentication for caGrid, user migration, new caGrid user creation, etc., as shown in Table 2-1 above.

The *CGMMManagerImpl* class implements the CGMMManager interface. Developers can easily incorporate the service into their host applications with simple configuration and coding changes to their applications.

Importing the CGMM Authentication API

To use the CGMM API's CGMMManager, add the last two (highlighted) import statements to the action classes, as shown below:

```
import gov.nih.nci.security.cgmm.CGMMManager;
import gov.nih.nci.security.cgmm.CGMMManagerImpl;
import gov.nih.nci.security.cgmm.beans.CGMMUser;
import gov.nih.nci.security.cgmm.exceptions.CGMMException;
import gov.nih.nci.security.cgmm.exceptions.CGMMConfigurationException;
import gov.nih.nci.security.cgmm.exceptions.CGMMConfigurationException;
import gov.nih.nci.security.cgmm.exceptions.CGMMInputException;
```

Obtaining the CGMMManager

The sample shown below provides example code to use the CGMM API - CGMMManager class in the 'sampleHostApplication' host application:

```
CGMMManager cgmmManager = null;
try {
    cgmmManager = new CGMMManagerImpl();
} catch (CGMMConfigurationException e) {
    System.out.println("ERROR Unable to obtain
CGMMManager");
}
```

Authenticating Users

The sample shown below provides example code for authenticating CSM users in the 'sampleHostApplication' host application.

```
String username = Form.getUsername();
String password = Form.getPassword();
//perform CSM Login
try{
    cgmmManager.performCSMLogin(username, password);
} catch (CGMMException e1) {
    System.out.println("ERROR Unable to perform CSM login");
}
```

Migrating Users

The sample shown below provides example code for migrating users in the 'sampleHostApplication' host application.

```
String userIDCSM = Form.getUsername();
String userIDGrid = Form.getGridID();
//perform Migration
try{
    boolean isMigrated = cgmmManager.isUserMigrated(username);
    if(!isMigrated)
        cgmmManager.migrateCSMUserIDToGridID(userIDCSM,
        userIDGrid);
} catch (CGMMException e1) {
    System.out.println("ERROR Unable to migrate the user.");
}
}
```

Integrating Auto Start SyncGTS servlet

To integrate the *StartSyncGTSServlet* in the host application, add the configuration shown in the example below to the `web.xml` file of the host application.

This configuration is required since it is the only way to ensure the server of the host application is in sync with the caGrid Trust Fabric before invoking any secured caGrid Services.

```
<servlet>
    <servlet-name>Start Auto Sync GTS </servlet-name>
    <servlet-class>
        gov.nih.nci.security.cgmm.util.StartSyncGTSServlet
    </servlet-class>
    <load-on-startup>2</load-on-startup>
</servlet>
```

Configurations for CGMM API

For successful integration of CGMM API into a host web application, the following configuration files must be configured correctly. Table 2-2 below shows the configuration files and changes needed for CGMM.

Configuration File	Description
<code>Cgmm-properties.xml</code>	<p>Required to specify the CGMM information, Host Application information and Authentication Service/Dorian information.</p> <p>Sample provided in Appendix B, Sample CGMM Properties File on page 45.</p> <p>Refer the <code>cgmm-property.xsd</code> shown in Appendix A for more information.</p> <p>The CGMMManager retrieves this file based on the System property <code>gov.nih.nci.security.cgmm.properties.file</code>.</p>
<code>Sync-description.xml</code>	<p>Required for the <code>StartSyncGTSServlet</code>.</p> <p>Refer to the sample provided in Appendix C for more information.</p> <p>The CGMMManager retrieves this file based on the System property <code>gov.nih.nci.security.cgmm.syncgts.file</code>.</p>
<code>Cgmm.login.config</code>	<p>Required to configure the CSM Authentication part of the CGMMManager API.</p> <p>Specifies the Login Module to be used by the CGMMManager (that internally uses CSM AuthenticationManager) to authenticate CSM users.</p> <p>The CGMMManager retrieves this file based on the System property <code>gov.nih.nci.security.cgmm.login.config.file</code>.</p> <p>NOTE: If the JBoss <code>login-config.xml</code> is configured with Login Module for the host application, then the System property <code>gov.nih.nci.security.cgmm.login.config.file</code> is ignored.</p>

Configuration File	Description
<p>ApplicationSecurity Config.xml</p>	<p>Required to configure the CSM Authorization part of the CGMMManager API used to migrate CSM users or obtain CSM User information. This file points to a hibernate.cfg.xml file for the host application. Refers to the <<name>>.hibernate.cfg.xml based on the specified path. The CGMMManager retrieves this file based on the System property gov.nih.nci.security.configFile.</p>
<p><<name>>.hibernate. cfg.xml</p>	<p>Required, along with ApplicationSecurityConfig.xml file noted above. It points to the CSM Schema for the host application. Replace <<name>> with the host application context name.</p>

Table 2-2 CGMM Configuration Files

Chapter 3 Using the CGMM Tool

The CGMM Tool is a web application that, on behalf of the host application, allows authentication of CSM/caGrid users, migration of a CSM user account to a caGrid user account, and/or creation of new caGrid accounts for users.

The CGMM tool is configurable and was created considering customizations by/for the host applications. The CGMM tool involves low level of effort for modification and configuration required by the host applications. The CGMM API, on the other hand, allows full integration of CGMM features programmatically, thus not requiring the use of CGMM Tool.

This chapter demonstrates the implemented CGMM workflows and scenarios followed by the configurable features of the CGMM Tool.

Workflows

The CGMM Tool allows multiple scenarios/workflows based on the User. The user may or may not have CSM account. The user also may or may not have a caGrid Account. Based on that, there are two primary scenarios with underlying situations addressed by the CGMM Tool:

1. User logs in with CSM account and
 - a. User has a caGrid account.
 - b. User does not have a caGrid account.
2. User logs in with caGrid account and
 - a. User has already been migrated.
 - b. User has a CSM account.
 - c. User does not have a CSM account.

NOTE: The CGMM tool DOES NOT addresses the scenario where a User does not have a CSM (local) Account and does not have a caGrid account. In this case, the host application needs to address this scenario.

The sections that follow look at the user interface workflow of the CGMM by going through each of the scenarios mentioned above. Figure 3-1 below shows the CGMM Tool Home page.

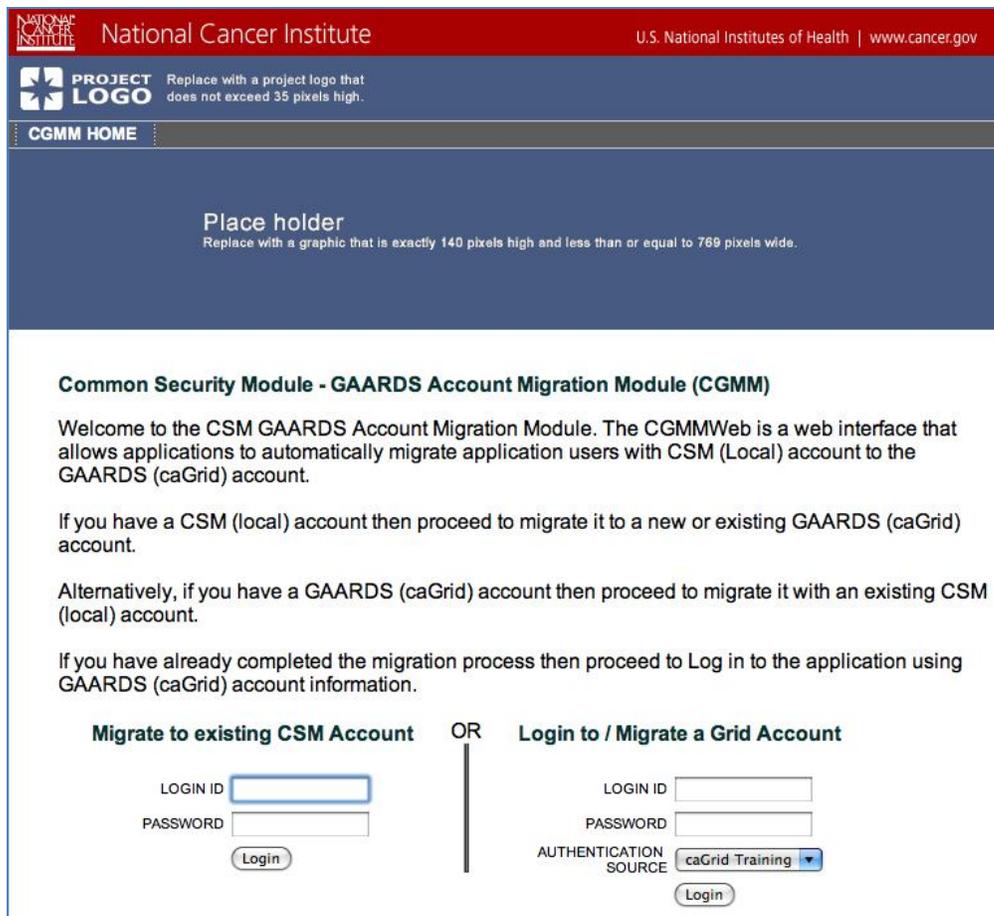


Figure 3-1 CGMM Home Page

The home page provides details and basic instructions to the user regarding how to proceed using the tool, depending on their situation.

Workflow Scenario 1: User Logs In with CSM Account

In this scenario, the User has the CSM account. The user logs in by providing their username and password and clicking on the Login button.

If the Login Id or Password is invalid, the CGMM tool shows an error.

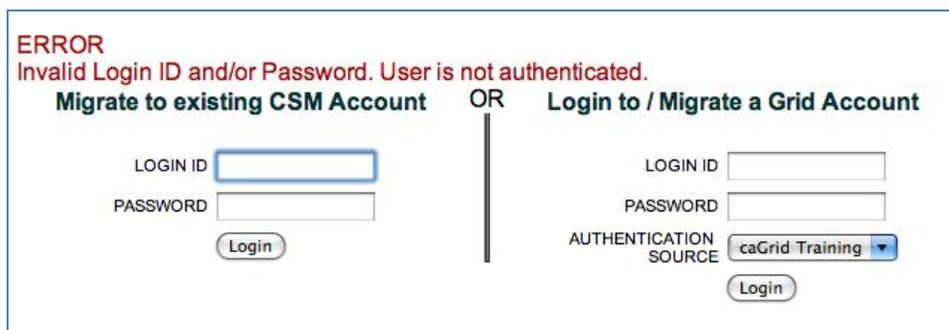


Figure 3-2 CGMM - CSM Login Error

If the Login Id and password are valid, the CGMM tool takes the user to CSM to GAARDS Account Migration page. In this page, the tool allows the user to either login using existing caGrid account or create a new caGrid account.

CGMM HOME

Place holder
Replace with a graphic that is exactly 140 pixels high and less than or equal to 769 pixels wide.

CSM to GAARDS Account Migration

This screen allows the User to migrate to a GAARDS (caGrid) account.

If you have a GAARDS (caGrid) account already then login using the caGrid Login ID and Password.

If you do not have any GAARDS (caGrid) account then proceed to create a new caGrid account by clicking on the 'Create a New caGrid Account' button. After creating a new caGrid account a migration confirmation screen will provide an option to migrate the newly created caGrid account.

Migrate a Grid Account OR **Create a new Grid Account**

LOGIN ID

PASSWORD

AUTHENTICATION SOURCE

Dont have a Grid Account?
Click the Create new Grid Account button to proceed.

Figure 3-3 CSM Login success page/Grid Login Page

Scenario 1-a: User Has caGrid Account

If the user already has an existing caGrid account, they can proceed to migrating to using their caGrid account by providing their Login ID and Password, and selecting the appropriate Authentication Source (Authentication Service).

User logs in with caGrid Login ID and password

After the user enters their caGrid login credentials and clicks **Login**, the CGMM Tool validates the caGrid account against the provided Authentication Source.

If the credentials are valid, the CGMM Tool displays the Confirm Migration screen to the user.

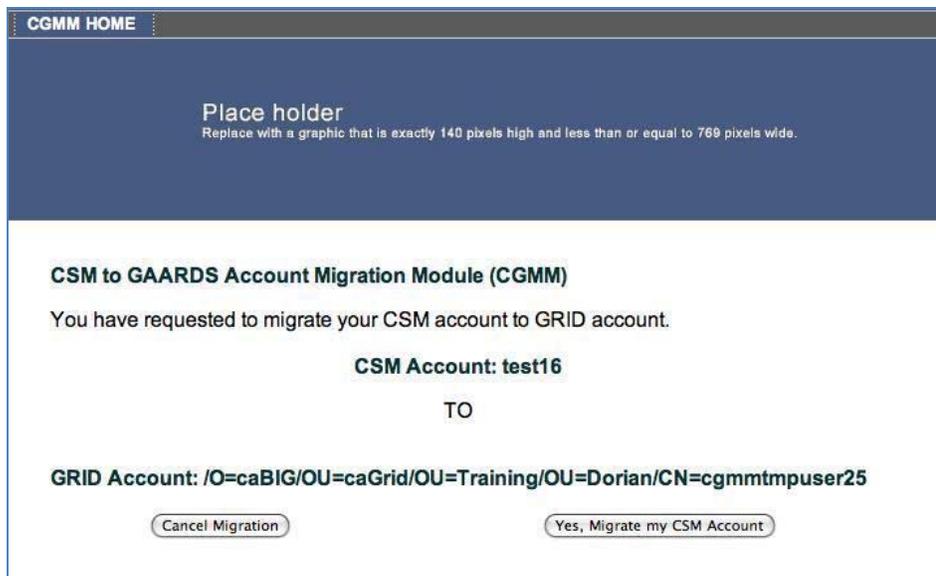


Figure 3-4 CSM to GAARDS Account Migration Page

User Chooses to Migrate His/Her Account

On the migration confirmation page, the user has the option to cancel the migration or confirm it.

When the user selects to migrate by clicking the **Yes, Migrate my CSM Account** button, CGMM migrates the CSM account to the caGrid account in the CSM Schema of the host application. CGMM will also mark the user as migrated.

Once the migration process is complete, the CGMM Tool takes the user to the migration confirmation page. The user now has the only option to log into the host application.

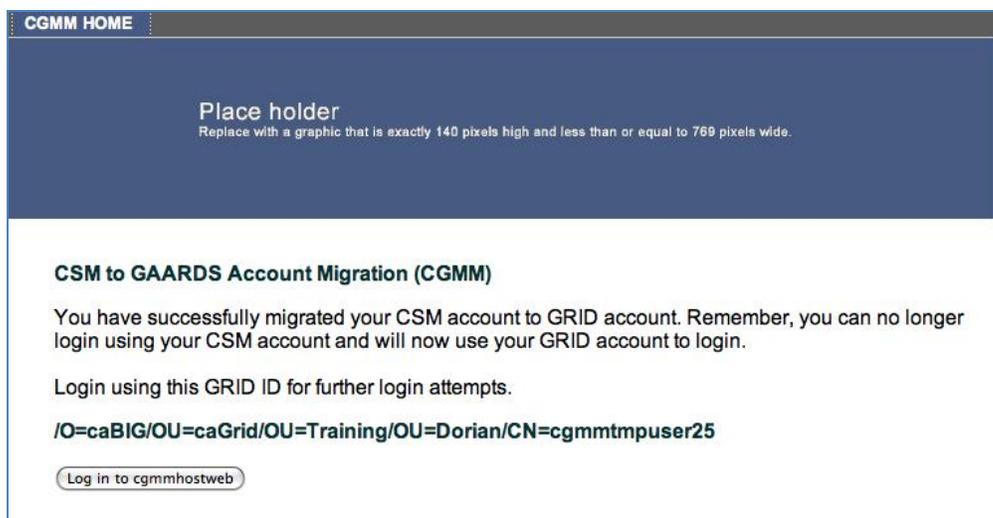


Figure 3-5 Migration Complete Page

When the user clicks the **Log in to <<Host Application Name>>** button, the CGMM proceeds to log in the user using the caGrid account information. The CGMM tool then populates the HTTP Request with the caGrid user information and the user's Grid Proxy as request attributes, and forwards the request to the Host application. This request is forwarded to the Host Applications User Home page, specified in the CGMM properties configuration. The CGMM then relinquishes control to the Host application.

If the request is accepted, the user is forwarded by the CGMM to the Host application User Home page.



Figure 3-6 Host Application User Home Page (migration complete)

The above figure shows the User Home page for the 'HostWeb' web application, shown as a reference implementation.

Scenario 1-b: User Does Not Have caGrid Account

If the user has a CSM login but does not have an existing caGrid account, the user can proceed to obtain a new caGrid account by selecting the Create New caGrid Account button. The Create new caGrid Account form appears.

CGMM HOME

Please provide details to create a new caGRID account. Click submit to attempt creation of new account.

Note: All fields are required.

Create new caGRID Account	
First Name	<input type="text" value="First27"/>
Last Name	<input type="text" value="Last27"/>
Username	<input type="text" value="cgmmtmpuser47"/>
Password	<input type="password" value="*****"/>
Email	<input type="text" value="cgmmtmpuser47"/>
Phone	<input type="text" value="1234567890"/>
Organization	<input type="text" value="nci"/>
Street Address 1	<input type="text" value="address 1"/>
Street Address 2	<input type="text" value="address 2"/>
City	<input type="text" value="Rockville"/>
State	<input type="text" value="MD"/>
Postal Code	<input type="text" value="20852"/>
Country	<input type="text" value="US"/>

Figure 3-7 New caGrid Account Form

The User must provide all the information requested to proceed.

After completing all of the fields, the user must click **Submit**. An account details page appears, asking the user to review the details entered into the form for creating the new caGrid account.

CGMM HOME

The new caGrid Account details are shown below.

New caGrid Account Details

First Name	First27
Last Name	Last27
Username	cgmmtmpuser47
Password	Abcdefgh123!
Email	cgmmtmpuser47@tmp.gov
Phone	1234567890
Organization	nci
Street Address 1	address 1
Street Address 2	address 2
City	Rockville
State	MD
Postal Code	20852
Country	US

[Confirm Migration](#)

Figure 3-8 New caGrid account information confirmation page

After confirming the details, the user must click **Confirm Migration**.

The CGMM attempts to create a new caGrid (Dorian) account with the form details provided by the user. The CGMM obtains the Dorian URL from the CGMM Properties configuration file.

If the account creation is successful, the CGMM tool returns a complete/success page.

CGMM HOME

Place holder
Replace with a graphic that is exactly 140 pixels high and less than or equal to 769 pixels wide.

CSM to GAARDS Account Migration Module (CGMM)

You have requested to migrate your CSM account to GRID account.

CSM Account: test27

TO

GRID Account: /O=caBIG/OU=caGrid/OU=Training/OU=Dorian/CN=cgmmtmpuser47

[Cancel Migration](#) [Yes, Migrate my CSM Account](#)

Figure 3-9 Account creation complete/success page

At this point, the user has the option to cancel the migration or select to migrate their CSM account to their newly created caGrid account.

When the user selects to migrate by clicking the **Yes, Migrate my CSM Account** button, CGMM migrates the CSM account to the new caGrid account in the CSM Schema of the host application. CGMM will also mark the user as migrated.

Once the migration process is complete, the CGMM Tool takes the user to the migration confirmation page. The user now has the option to log into the host application.

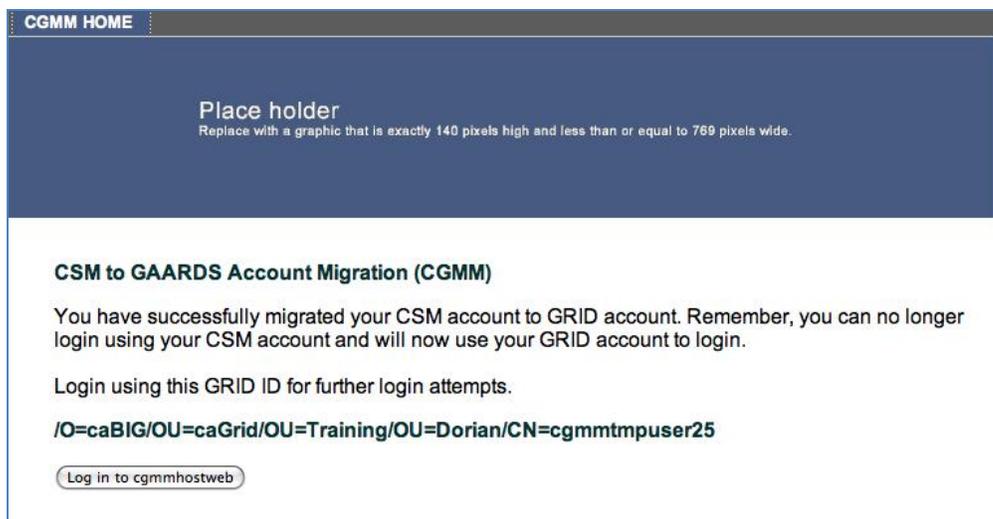


Figure 3-10 Migration complete page

When the user clicks the **Log in to <<Host Application Name>>** button, the CGMM proceeds to log in the user using the caGrid account information. The CGMM tool then populates the HTTP Request with the caGrid user information and the user's Grid Proxy as request attributes, and forwards the request to the Host application. This request is forwarded to the Host Applications User Home page that is specified in the CGMM properties configuration. The CGMM then relinquishes control to the Host application.

If the request is accepted, the user is forwarded by the CGMM to the Host application User Home page (as shown in Figure 3-6 above).

Workflow Scenario 2: User Logs In with caGrid Account

If the User has a caGrid account, they can login by providing their username, password, and then selecting the appropriate Authentication Source from the drop-down list. The User then clicks **Login**.

If the Login Id or Password is invalid, the CGMM tool displays an error.

Figure 3-11 CGMM - caGrid Login Error

Scenario 2-a: User Is Already Migrated

After entering their caGrid login credentials, the CGMM tool validates the user's caGrid Login ID and password. The CGMM Tool also verifies whether the caGrid User ID exists as a migrated user in the CSM Schema of the host application. If the user is already migrated, then the CGMM Tool populates the HTTP Request with user's details and Grid Proxy, and then forwards the request to the host application's User Home page as shown in Figure 3-6 above.

Scenario 2-b: User Has CSM Account

After entering their caGrid login credentials, the CGMM tool validates the user's caGrid Login ID and password.. The CGMM Tool also verifies whether the caGrid User ID exists as a migrated user in the CSM Schema of the host application.

If the user has not been migrated, the tool presents the user with a CSM Login Page in which they can enter their CSM login credentials or create a new CSM account.



GAARDS to CSM Account Migration

This screen allows the User to migrate to an existing CSM (local) account or proceed to the host application to create a new CSM (local) account.

If you have a CSM (local) account already then login using the CSM Login ID and Password.

If you do not have any CSM (local) account then proceed to create a new CSM (local) account by clicking on the 'Create a New CSM Account' button.

Figure 3-12 caGrid Login Success - CSM Login Page

Since in this scenario the user has an existing CSM account, the user can proceed to migrate CSM account by providing their CSM Login ID, Password, and clicking **Login**.

User Logs In with CSM Login ID and Password

After the user provides their CSM login credentials and clicks **Login**, the CGMM Tool validates the credentials provided by the user. If the credentials are valid, the CGMM Tool displays the Confirm Migration screen.

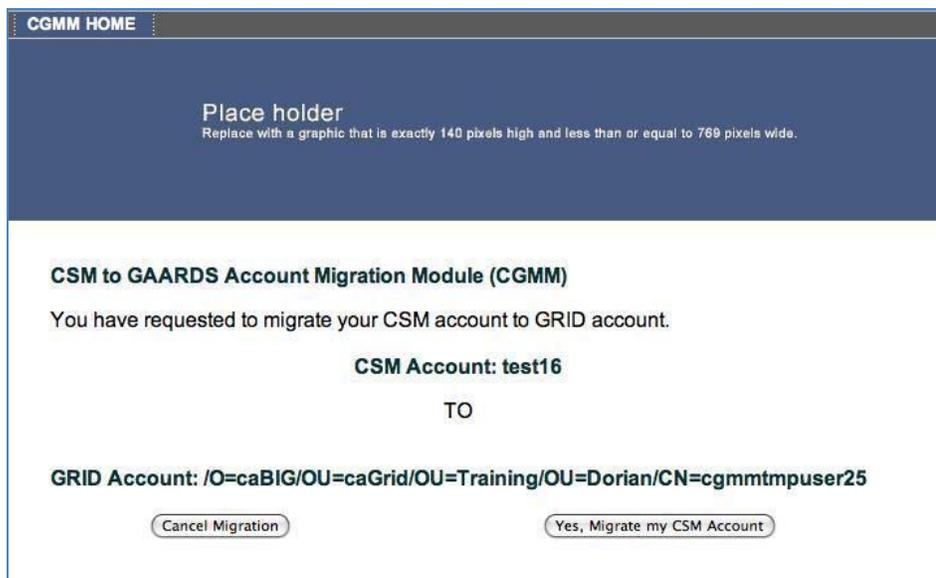


Figure 3-13 CSM to GAARDS Account Migration Page

If the user selects **Yes, Migrate my CSM Account**, CGMM proceeds to migrate the CSM account with the caGrid account. If the migration is successful, the CGMM tool shows the migration complete/success page.

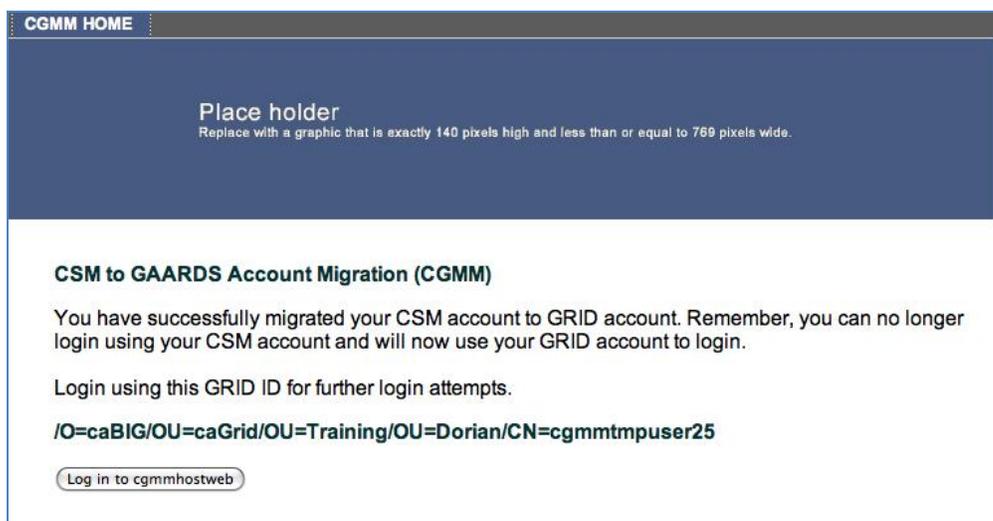


Figure 3-14 Migration Complete Page

When the user clicks the **Log in to <<Host Application Name>>** button, the user is logged in and is forwarded by the CGMM to the Host application User Home page.



Figure 3-15 Migration Complete Page - Host Application User Home Page

The above figure shows the User Home page for the 'HostWeb' web application, shown as a reference implementation.

Scenario 2-c: User Does Not Have a CSM Account

If the user has logged in with their caGrid account but does not have a CSM account, when they are presented with the CSM login page, they are left with the option to request the creation of a new CSM account for the host application.

 A screenshot of a web page titled 'CGMM HOME'. It contains a 'Place holder' with instructions: 'Replace with a graphic that is exactly 140 pixels high and less than or equal to 769 pixels wide.' Below this is a section 'GAARDS to CSM Account Migration' with explanatory text. At the bottom, there are two options: 'Migrate to existing CSM Account' with input fields for 'LOGIN ID' and 'PASSWORD' and a 'Login' button; and 'Create a new CSM Account' with a 'Create New CSM Account' button. A note says: 'Dont have a local (CSM) Account?. Click Create New CSM Account button to proceed to the applications new User account creation workflow.'

Figure 3-16 caGrid Login Success - CSM Login Page

When the user selects **Create New CSM Account**, the CGMM tool populates the HTTP request with caGrid User account and the user's Grid Proxy, and forwards the request to the Host application to relieve control. The CGMM tool then forwards the request to the host application's New CSM User Creation page. The CGMM obtains the context and URL for this page from the CGMM properties configuration file.

Configuring the CGMM Tool

CGMM Tool is designed to be customizable to allow host applications to implement the workflows however they decide to do so. The following are the customizations and configurations allowed for the CGMM tool:

1. Configurable Look and Feel

The new caGrid User creation feature can be enabled or disabled based on the needs of the host application. This is achieved by configuring the *cgmm-information* section of the *cgmm-properties.xml* file with following:

- a. Set the `<cgmm-new-grid-user-creation-disabled>` element to `true`
- b. Set the `<cgmm-new-grid-user-creation-host-redirect-uri>` element to the host application context relative URI.

2. CGMM Information

The CGMM information configuration allows the following:

- a. Changing the CGMM tool's context name.
- b. Enable/disable the Auto Start SyncGTS Servlet
- c. Change the name of the *cgmm.login.config* file.
- d. Enable/disable the new caGrid User feature
- e. If disabled, provide the host application the new caGrid user page URL.

3. Configurable CaGrid Identity Providers for Authentication

The list of caGrid Identity providers is configurable via the *cgmm-properties.xml* file.

4. Host Information

The Host information customization allows the following:

- a. Configurable Host application web context name.
- b. Configurable name of the Host application.
- c. Configurable host applications Home page URL.
- d. Configurable host applications User Home Page URL.
- e. Configurable host applications new CSM user page URL.

5. Authentication Service/Dorian Information

The Authentication Service list allows specifying one or more Authentication Services to use for authentication purpose. The Dorian information, for each Authentication Service, can be used to create accounts, etc.

6. SyncGTS Configuration

The *sync-description.xml* configuration file allows specifying the GTS Service URI, Trusted Authority filters, Excluded CA's, etc.

Chapter 4 CGMM Installation and Deployment

This chapter provides details regarding the contents of the CGMM release. Topics in this chapter include:

- [Release Contents](#) on page 34.
- [Installation Pre-Requisites](#) on page 34.
- [Deployment Checklist](#) on page 36.
- [Deployment Steps](#) on page 37.

Figure 4-1 shows a diagram of a CGMM deployment and is provided as a reference for the information provided throughout the rest of this chapter.

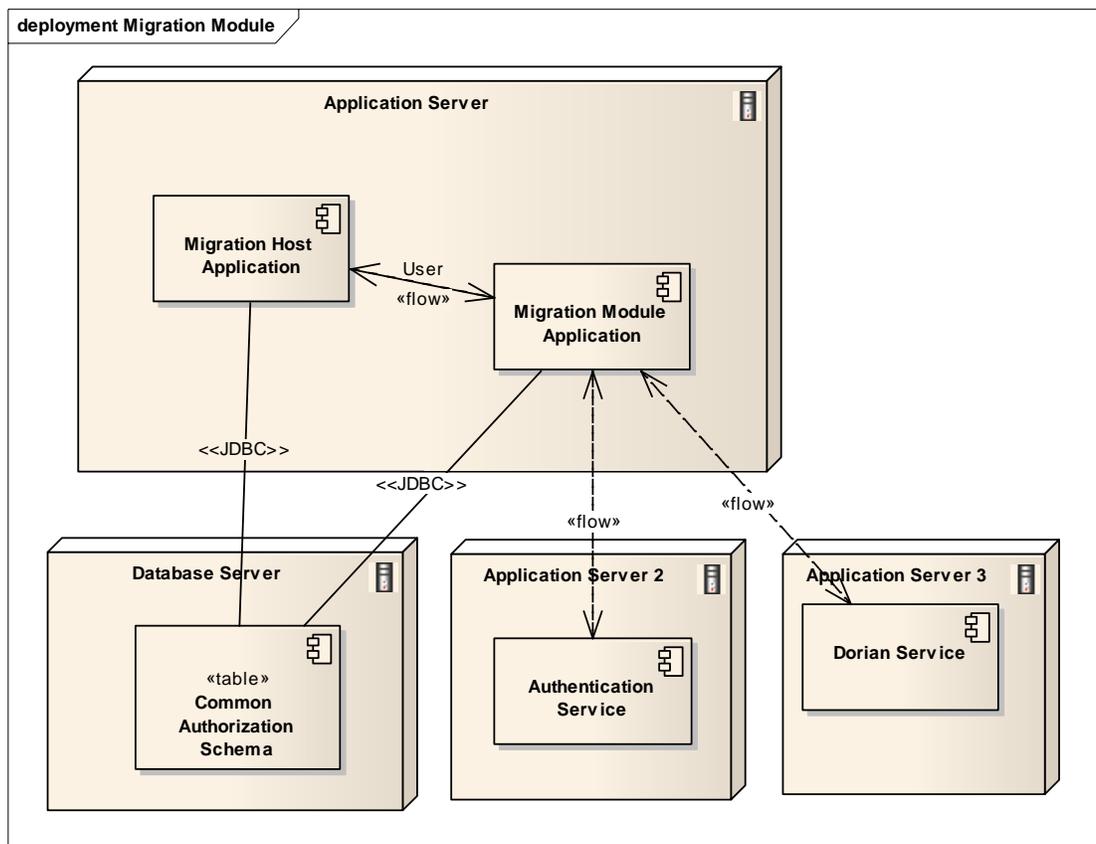


Figure 4-1 CGMM Deployment Diagram

NOTE: In order for the CGMM Tool to function properly, the environment setup detailed in the [Installation Pre-Requisites](#) section of this chapter has to be made available.

Release Contents

The CGMM is released both as a CGMM API Jar file and as a compressed web application in the form of a WAR (Web Archive) File. Along with the JAR and WAR files, the release includes sample configuration files, designed to help developers configure the CGMM with their application(s). The CGMM Filter jar file is also made available.

The CGMM Release contents can be found in the `CGMM.zip` file found on the NCICB GForge website in the Security projects File Tab:

https://gforge.nci.nih.gov/frs/?group_id=12.

The CGMM Release contents include the files listed and described in the following table:

File	Description
<code>cgmmweb.war</code>	The CGMM Tool WAR file.
<code>Cgmmapi.jar</code>	The CGMM API Jar file.
<code>Cgmmfilter.jar</code>	The CGMM Filter jar file.
<code>Cgmm-properties.xml</code>	The CGMM properties configuration file.
<code>ApplicationSecurityConfig.xml</code>	The CSM Security Configuration file for various applications. For CGMM this file names and points to the Hibernate configuration file that will be used by the <code>CGMMManager</code> of CGMM for obtaining <code>CSM AuthenticationManager/AuthorizationManager</code> .
<code>Cgmmweb.hibernate.cfg.xml</code>	This is the Hibernate configuration file pointed out by the <code>ApplicationSecurityConfig.xml</code> file for CSM. It is used to specify the Database connection properties or the Data Source name to be used for the Host Application Name.
<code>cgmm.login.config</code>	The <code>login.config</code> file to be used for obtaining the <code>LoginModule</code> for the Host application. The <code>login.config</code> file should be used to configure the login configuration for the Host application name.
<code>sync-description.xml</code>	The configuration file used by the <code>SyncGTS</code> servlet to sync the <code>caGrid</code> Trust fabric. This is required for <code>caGrid</code> Authentication purposes.

Table 4-1 CGMM Release Contents

Installation Pre-Requisites

The installation pre-requisites described in the sections that follow *must* be performed before the CGMM Tool can be installed.

Refactoring Host Application

The Host application must implement the following:

1. Add CGMM Filter to intercept all User requests. Shown below is the `Web.xml` configuration needed to add CGMM Filter.

```
<filter>
  <filter-name>CGMigrationFilter</filter-name>
  <filter-class>
    gov.nih.nci.security.cgmm.filters.CGMigrationFilter
  </filter-class>
  <init-param>
    <param-name>CGMM_APPLICATION_CONTEXT</param-name>
    <param-value>cgmmweb</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>CGMigrationFilter</filter-name>
  <url-pattern>/secured/*</url-pattern>
</filter-mapping>
```

2. Identify the `cgmm-properties.xml` configuration details for Host information section.

A sample configuration is shown below and in [Appendix B, Sample CGMM Properties File](#) on page 45. Refer also to the `cgmm-properties.xsd` shown in [Appendix A](#) for more details about each configuration element.

```
<host-application-information>
  <host-context-name>cgmmhostweb</host-context-name>
  <host-application-name-for-csm>sampleHostApplication</host-application-name-for-csm>
  <host-public-home-page-url>/public/publicHome.jsp</host-public-home-page-url>
  <host-user-home-page-url>/secured/userHomePage.jsp</host-user-home-page-url>
  <host-new-local-user-creation-url>/public/newLocalUserCreation.jsp
    </host-new-local-user-creation-url>
</host-application-information>
```

caGrid Security Infrastructure

1. Identify the Authentication Service(s) that will be used for authenticating caGrid users.
2. Identify the Dorian service that will be used to obtain grid proxy, create new caGrid user accounts, etc.
3. Identify the `sync-description.xml` configuration information. For more details, see the sample configuration file provided in [Appendix C](#) on page 47.
4. Identify the `cgmm-properties.xml` configuration details for Authentication Service and Dorian Service information.

A sample configuration is shown below. Refer also to the `cgmm-properties.xsd` shown in [Appendix A](#) for more details about each configuration element.

```
<authentication-service-list>
<authentication-service-information>
<service-name>caGrid Training</service-name>
<service-url> https://dorian.training.cagrid.org:8443/wsrf/services/cagrid/Dorian</service-url>
<dorian-information>
  <service-url>https://dorian.training.cagrid.org:8443/wsrf/services/cagrid/Dorian</service-url>
  <proxy-lifetime-hours>12</proxy-lifetime-hours>
  <proxy-lifetime-minutes>0</proxy-lifetime-minutes>
  <proxy-lifetime-seconds>0</proxy-lifetime-seconds>
  <proxy-delegation-path-length>3</proxy-delegation-path-length>
</dorian-information>
</authentication-service-information>
</authentication-service-list>
```

Identify Configuration Parameters for CGMM

1. Determine if the new caGrid User creation feature of the CGMM Tool is desired.
2. If the new caGrid user creation feature is to be disabled, configure the `cgmm-information` section of the `cgmm-properties.xml` file with following:
 - a. Set the `<cgmm-new-grid-user-creation-disabled>` element to `true`
 - b. Set the `<cgmm-new-grid-user-creation-host-redirect-uri>` element with host application context relative URI.

Deployment Checklist

Before deploying the CGMM, verify that the following environment and configuration conditions are met. The software and access credentials/parameters are required.

Host Application Environment

- JBoss 4.0 Application Server
- MySQL 4.0 OR Oracle 9i Database Server (with an account that can create databases)
- Host Application utilizing the CGMM Filter.
- CSM v4.1 Schema with existing Users.

CGMM Release Components

- CGMM Properties configuration file
- Sync Description configuration file
- ApplicationSecurityConfig.xml Security configuration for CGMM
- JAAS Login Module Configuration for 'sampleHostApplication' Application.

caGrid Environment

- caGrid 1.2 software is installed
- Dorian Service is available for creation of new Grid User accounts.
- Authentication Service(s) available to authenticate Grid users.
- SyncGTS to sync with Trust Fabric.
- Host Certificate is available for the Server hosting the application server.

Deployment Steps

Before deploying CGMM, verify that the installation prerequisites have been completed and that the deployment checklist is complete.

Step 1: Deploy cgmmweb.war file

Copy the `cgmmweb.war` file into the deployment directory of JBoss, located at: `{jboss-home}/server/default/deploy/`.

Step 2: Deploy Host Application with CGMM Filter

Copy the host application's WAR file into the deployment directory of Jboss, located at: `{jboss-home}/server/default/deploy/`.

Step 3: Configure System Properties

Set the System properties for the configuration files.

In Jboss, modify the `Jboss_home/server/default/deploy/properties-service.xml`. A sample configuration is shown below:

```
<attribute name="Properties">
gov.nih.nci.security.cgmm.syncgts.file =
    <<path to>>/sync-description.xml
gov.nih.nci.security.cgmm.properties.file =
    <<path to>>/cgmm-properties.xml
gov.nih.nci.security.configFile =
    <<path to>>/ApplicationSecurityConfig.xml
gov.nih.nci.security.cgmm.login.config.file =
    <<path to>>/cgmm.login.config
</attribute>
```

Step 4: Configure SyncGTS

Configure the URLs for Slave/Master GTS. Refer also to [Appendix C, Sample Sync Description File](#) on page 47.

Step 5: Configure the CGMM Properties File

For a description of the elements, see [Appendix A, CGMM Properties XSD File](#) on page 41

Example:

```
<host-application-name-for-csm>sampleHostApplicationContextName</host-
application-name-for-csm>
```

Step 6: Configure the CSM Application Security Configuration File

Configure `ApplicationSecurityConfig.xml` as follows:

- Change the `<context-name>` element to the Host application context name. For example:

```
<context-name>sampleHostApplicationContextName </context-name>
```
- Change the `<hibernate-config-file>` element to point to the Hibernate configuration file. For example:

```
<hibernate-config-file><<path to>>/cgmmweb.hibernate.cfg.xml</hibernate-config-file>
```

Configure `<<hostApplicationName>>.hibernate.cfg.xml` to:

- Configure the Database Connection Properties or Datasource for the application.

Step 7: Configure the Jboss JAAS Login Parameters

In order to configure the CGMM to authenticate CSM users, create an entry in the `login-config.xml` file of Jboss as shown below. This entry configures a login-module against the host application context.

```
<application-policy name = "sampleHostApplication">
<authentication>
<login-module
    code="gov.nih.nci.security.authentication.loginmodules.RDBMS
LoginModule"
    flag = "sufficient">
<module-option name="driver"><<Database Driver>></module-option>
<module-option name="url"><<Database URL>></module-option>
<module-option name="user"><<DB Username>></module-option>
<module-option name="passwd"><<DB Password>></module-option>
<module-option name="query">
    SELECT * FROM csm_user WHERE login_name=? and
password=?</module-option>
<module-option name="encryption-enabled">YES</module-option>
    </login-module></authentication>
</application-policy>
```

The location of this file is: `{jboss-home}/server/default/conf/login-config.xml`.

Alternatively, the JAAS configuration can be done via the `cgmm.login.config` configuration file by performing the following:

- Rename the `cgmm.login.config` file to the value specified System property `gov.nih.nci.security.cgmm.login.config.file`.
- Modify the `login.config` name to the Host Application Name.
- Point to the Host application Schema (CSM 4.1 Schema of the Host application).

Step 8: Start Jboss

Once the deployment and configuration is completed, start JBoss. Check the logs to confirm there are no errors while the CGMM Web application and host application are deployed on the server.

Once the Jboss server has completed deployment, open a browser to access the host applications secured login page. The URL is:

`http://<<jboss-server>>/<<host_application_context>>`

Where `<<jboss-server>>` is the IP or the DNS name of Jboss Server and `<<host_application_context>>` is the context name of the host application.

The Host application should forward the control to CGMM Tool's login screen.

NOTE: In case of any errors, follow a debugging and troubleshooting procedure to diagnose and solve the issues. For more information refer the CGMM FAQ page of the CSM Wiki located at: <https://wiki.nci.nih.gov/x/4wBB>.

Appendix A CGMM Properties XSD File

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:element name="authentication-service-information">
    <xs:annotation>
      <xs:documentation>Element allows specifying required
Authentication Information. Please refer the caGrid Wiki for details regarding
Authentication Service.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="service-name"/>
        <xs:element ref="service-url"/>
        <xs:element ref="dorian-information"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="authentication-service-list">
    <xs:annotation>
      <xs:documentation>Element allows specifying a list of
Authentication.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="authentication-service-information"
maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="dorian-information">
    <xs:annotation>
      <xs:documentation>element allows specification of caGrid Dorian
information. Please refer the caGrid Wiki for details regarding Dorian. </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="service-url"/>
        <xs:element ref="proxy-lifetime-hours"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

```

        <xs:element ref="proxy-lifetime-minutes"/>
        <xs:element ref="proxy-lifetime-seconds"/>
        <xs:element ref="proxy-delegation-path-length"/>
    </xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="cgmm-information">
    <xs:annotation>
        <xs:documentation>element allows specification of CGMM related.
            </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="cgmm-context-name"/>
            <xs:element ref="cgmm-login-config-file-name"/>
            <xs:element ref="start-auto-syncgts"/>
            <xs:element ref="cgmm-new-grid-user-creation-disabled"/>
            <xs:element ref="cgmm-new-grid-user-creation-host-redirect-
uri"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="host-application-information">
    <xs:annotation>
        <xs:documentation>element allows specification of Host Application
information.
            </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="host-context-name"/>
            <xs:element ref="host-application-name-for-csm"/>
            <xs:element ref="host-public-home-page-url"/>
            <xs:element ref="host-user-home-page-url"/>
            <xs:element ref="host-new-local-user-creation-url"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="cgmm-new-grid-user-creation-disabled" type="xs:string">
    <xs:annotation>
        <xs:documentation>element indicates if the New Grid User Creation
is disabled for this installation of CGMM. A of true indicates the particular workflow is. If
disabled the new-grid-user-creation-host-redirect-url is. The value of false indicates that the
workflow not disabled. The new-grid-user-creation-host-redirect-url is to have valid content.
            </xs:documentation>
    </xs:annotation>

```

```

    </xs:element>
    <xs:element name="cgmm-new-grid-user-creation-host-redirect-uri"
type="xs:string" nillable="true">
      <xs:annotation>
        <xs:documentation>element allows specifying the Hosts Redirect
URL the New Grid User creation workflow is successfully. If this workflow is disabled,
then the this is ignored.
        </xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="cgmm-context-name" type="xs:string">
      <xs:annotation>
        <xs:documentation>Web application context name of CGMM Web .
The default value is cgmmweb
        </xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="cgmm-login-config-file-name" type="xs:string">
      <xs:annotation>
        <xs:documentation>JAAS Login Config file name. This file consists
of the Authentication configuration necessary for of CSM users. If the
security.auth.login.config JAAS property is set in then this element is ignored and the
Module Configuration for cgmmweb is obtained from particular Login Configuration.
        </xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="host-context-name" type="xs:string">
      <xs:annotation>
        <xs:documentation>
Web Application Context name of the Host Web
.This string value must match the web context
of the host application.
        </xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="host-application-name-for-csm" type="xs:string">
      <xs:annotation>
        <xs:documentation>
Application Name of the Host Web that is to
be used by CSM authentication and authorization.
This string value must match the of the host
application available in the CSM Schema.
        </xs:documentation>
      </xs:annotation>
    </xs:element>
    <xs:element name="host-public-home-page-url" type="xs:string"/>

```

```

<xs:element name="host-user-home-page-url" type="xs:string"/>
<xs:element name="host-new-local-user-creation-url" type="xs:string">
  <xs:annotation>
    <xs:documentation>
      element OPTIONAL allows specifying the URL for New
      User creation workflow of the Host application.
    </xs:documentation>
  </xs:annotation>
</xs:element>
<xs:element name="start-auto-syncgts" type="xs:string"/>
<xs:element name="service-name" type="xs:string"/>
<xs:element name="service-url" type="xs:anyURI"/>
<xs:element name="proxy-lifetime-hours" type="xs:integer"/>
<xs:element name="proxy-lifetime-minutes" type="xs:integer"/>
<xs:element name="proxy-lifetime-seconds" type="xs:integer"/>
<xs:element name="proxy-delegation-path-length" type="xs:integer"/>
<xs:element name="cgmm-properties">
  <xs:annotation>
    <xs:documentation>

```

Root Element of the CGMM Properties. This element specifying the CGMM information, Host Application and Authentication Service/Dorian

```

.
</xs:documentation>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="cgmm-information"/>
      <xs:element ref="host-application-information"/>
      <xs:element ref="authentication-service-list"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
</xs:schema>

```

Appendix B Sample CGMM Properties File

```
<?xml version="1.0" encoding="UTF-8"?>
<cgmm-properties xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="cgmm-properties.xsd">
  <cgmm-information>
    <cgmm-context-name>cgmmweb</cgmm-context-name>
    <cgmm-login-config-file-name>cgmm.login.config</cgmm-login-config-
file-name>
    <start-auto-syncgts>true</start-auto-syncgts>
    <cgmm-new-grid-user-creation-disabled>>false</cgmm-new-grid-user-
creation-disabled>
    <cgmm-new-grid-user-creation-host-redirect-
uri>/public/newGridUserCreation.jsp</cgmm-new-grid-user-creation-host-redirect-uri>
  </cgmm-information>
  <host-application-information>
    <host-context-name>cgmmhostweb</host-context-name>
    <host-application-name-for-csm>sampleHostApplication</host-application-
name-for-csm>
    <host-public-home-page-url>/public/publicHome.jsp</host-public-home-page-url>
    <host-user-home-page-url>/secured/userHomePage.jsp</host-user-home-page-url>
    <host-new-local-user-creation-url>/public/newLocalUserCreation.jsp</host-new-
local-user-creation-url>
  </host-application-information>
  <authentication-service-list>
    <authentication-service-information>
      <service-name>caGrid Training</service-name>
      <service-
url>https://dorian.training.cagrid.org:8443/wsrf/services/cagrid/Dorian</service-url>
      <dorian-information>
        <service-
url>https://dorian.training.cagrid.org:8443/wsrf/services/cagrid/Dorian</service-url>
        <proxy-lifetime-hours>12</proxy-lifetime-hours>
        <proxy-lifetime-minutes>0</proxy-lifetime-minutes>
        <proxy-lifetime-seconds>0</proxy-lifetime-seconds>
        <proxy-delegation-path-length>3</proxy-delegation-path-
length>
      </dorian-information>
    </authentication-service-information>
  </authentication-service-list>
</cgmm-properties>
```


Appendix C Sample Sync Description File

```
<ns1:SyncDescription xmlns:ns1="http://cagrid.nci.nih.gov/12/SyncGTS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <ns1:SyncDescriptor>
    <ns1:gtsServiceURI>https://slavegts.training.cagrid.org:8443/wsrp/services/cagrid/GTS</ns1:gtsServiceURI>
    <ns1:Expiration hours="12" minutes="0" seconds="0"/>
    <ns1:TrustedAuthorityFilter xsi:type="ns2:TrustedAuthorityFilter"
xmlns:ns2="http://cagrid.nci.nih.gov/8/gts">
      <ns2:Lifetime xsi:type="ns2:Lifetime">Valid</ns2:Lifetime>
      <ns2:Status xsi:type="ns2:Status">Trusted</ns2:Status>
    </ns1:TrustedAuthorityFilter>
    <ns1:PerformAuthorization>true</ns1:PerformAuthorization>
    <ns1:GTSIdentity>/O=caBIG/OU=caGrid/OU=Training Trust
Fabric/CN=host/slavegts.training.cagrid.org</ns1:GTSIdentity>
  </ns1:SyncDescriptor>
  <ns1:ExcludedCAs>
    <ns1:CASubject>O=caBIG,OU=caGrid,OU=Training Trust
Fabric,CN=caGrid Training Trust Fabric CA</ns1:CASubject>
  </ns1:ExcludedCAs>
  <ns1>DeleteInvalidFiles>>false</ns1>DeleteInvalidFiles>
  <ns1:CacheSize>
    <ns1:year>0</ns1:year>
    <ns1:month>1</ns1:month>
    <ns1:day>0</ns1:day>
  </ns1:CacheSize>
  <ns1:NextSync>600</ns1:NextSync>
</ns1:SyncDescription>
```


Appendix D Sample Install of CGMM with Reference Implementation

The steps provided in this Appendix will work as long as the steps are followed correctly. These steps will install the reference implementation *cgmmHostWeb* web application along with the *cgmmweb* web application.

Using these steps, a test environment can be setup to demonstrate how the CGMM Tool works with an existing Host application. The internal details of the CGMM Tool are beyond the scope of this guide. Refer the *CGMM Design Document* for more details.

NOTE: The paths and values used in the commands and configuration files are for example only.

1. Verify caGrid 1.2 is installed. The CAGRID_HOME variable should be set.

If caGrid 1.2 is not installed, install caGrid 1.2 using the caGrid Installer 1.2 (install the software only; no services are needed).

2. Verify ANT_HOME, JAVA_HOME, CAGRID_HOME, and GLOBUS_LOCATION are set as environment variables. If the variables are not set, set the variables as shown below.

At the command prompt, type the following and press **Enter** after each statement:

```
ANT_HOME=/usr/local/apache-ant-1.6.5
export ANT_HOME;
PATH=$PATH:/usr/local/apache-ant-1.6.5/bin
export PATH;
JAVA_HOME=/usr/jdk1.5.0_10
export JAVA_HOME;
GLOBUS_LOCATION=/usr/local/ws-core-4.0.3
export GLOBUS_LOCATION;
CAGRID_HOME=/hl/username/⟨⟨path where caGrid was installed⟩⟩
export CAGRID_HOME;
```

3. Verify caGrid 1.2 is configured to point to the Training Grid 1.2, as shown below:

At the command prompt, type the following and press **Enter** after each statement:

```
Cd $CAGRID_HOME
ant -Dtarget.grid=training-1.2 configure
```

4. Run SyncGTS as shown below.

At the command prompt, type the following and press **Enter** after each statement:

```
Cd $CAGRID_HOME/projects/syncgts
ant syncWithTrustFabric
```

5. Obtain Host Certificate for the machine.

This is a pre requisite and the instructions for obtaining the Host Credentials (certificate) is available from the following link:

http://www.caGrid.org/mwiki/index.php?title=Dorian:1.1:Administrators_Guide:Requesting_Host_Credentials

6. Deploy the `cgmmHostWeb.war` by putting the war file in the JBoss deployment folder: `{jboss-home}/server/default/deploy/`.
7. Deploy the `cgmmweb.war` by putting the war file in JBoss de deployment folder: `{jboss-home}/server/default/deploy/`.
8. Configure the CGMM and Host Application properties.
9. Configure System Properties, as shown below:

Modify the `{jboss-home}/server/default/deploy/properties-service.xml` and add the following properties:

```
gov.nih.nci.security.cgmm.syncgts.file = /usr/local/jboss-4.0.5.GA/server/default/cgmm_config/sync-description.xml
gov.nih.nci.security.cgmm.properties.file = /usr/local/jboss-4.0.5.GA/server/default/cgmm_config/cgmm-properties.xml
gov.nih.nci.security.configFile = /usr/local/jboss-4.0.5.GA/server/default/cgmm_config/ApplicationSecurityConfig.xml
gov.nih.nci.security.cgmm.login.config.file = /usr/local/jboss-4.0.5.GA/server/default/cgmm_config/cgmm.login.config
```

10. Configure JAAS Login Configuration Module as follows:

- o Rename the `cgmm.login.config` file to value specified System property `gov.nih.nci.security.cgmm.login.config.file`
- o Modify the name of the `cgmm.login.config` file to `sampleHostApplication.login.config`
- o Point to the CSM 4.1 Schema for the `sampleHostApplication`.

11. Configure the Sync GTS description configuration xml file.

This is required to sync the caGrid Trust Fabric with the Server's Keystore. The instructions on how to configure the `sync-description.xml` is available through the following link:

http://www.caGrid.org/wiki/GTS:1.2:Administrators_Guide:SyncGTS:Configuration

In addition, the sample `sync-description.xml` provided in [Appendix C](#) points to the caGrid Training 1.2

12. Configure CGMM Properties file.:

For description of the elements see the `cgmm-properties.xsd` in [Appendix A](#).

Use the contents of [Appendix B](#) to configure the `cgmm-properties.xml` file.

13. Configure `ApplicationSecurityConfig.xml` file as follows:

- o Modify the `<context-name>` to the Host application context name. For example:

```
<context-name>sampleHostApplication</context-name>
```

- o Modify the `<hibernate-config-file>` element to point to the hibernate configuration file. For example:

```
<hibernate-config-file>
/usr/local/jboss-
4.0.5.GA/server/default/cgmm_config/cgmmweb.hibernate.cfg.x
ml
</hibernate-config-file>
```

14. Configure the Database Connection Properties or Datasource for the application as follows:

- o Specify the Database connection properties in `cgmmweb.hibernate.cfg.xml` as shown below:

```
<property name="connection.username">root</property>
<property name = "connection.url">
jdbc:mysql://localhost:3306/csmauthschema_4_1
</property>
<property
name="dialect">org.hibernate.dialect.MySQLDialect</property>
<property name="connection.password">root</property>
<property
name="connection.driver_class">org.gjt.mm.mysql.Driver</proper
ty>
```

- o OR configure the datasource.

The sample `JBOSS_HOME/server/default/deploy/mysql-ds.xml` configuration is shown below:

```
<local-tx-datasource>
  <jndi-name>cgmmweb</jndi-name>
  <connection-
url>jdbc:mysql://localhost:3306/csm41</connection-url>
  <driver-class>org.gjt.mm.mysql.Driver</driver-class>
  <user-name>root</user-name>
  <password>root</password>
</local-tx-datasource>
```


Glossary

The following table contains a list of terms used in this document along with their definitions.

Term	Definition
Ant	Apache Ant is a Java-based build tool used to perform various build related tasks. For more information on how Ant is used within the SDK. See http://ant.apache.org/ for more information on Ant itself.
caGrid	The cancer Biomedical Informatics Grid, or caBIG [®] , is a voluntary virtual informatics infrastructure that connects data, research tools, scientists, and organizations to leverage their combined strengths and expertise in an open federated environment with widely accepted standards and shared tools. The underlying service oriented infrastructure that supports caBIG [®] is referred to as caGrid. See http://www.cagrid.org
Ehcache	Ehcache is a simple, fast and thread safe cache for Java that provides memory and disk stores and distributed operation for clusters. CSM uses ehcache in conjunction with Hibernate. See http://sourceforge.net/projects/ehcache for more information.
Globus Toolkit	The Globus [®] Toolkit is an open source software toolkit used for building grids. It is being developed by the Globus Alliance and many others all over the world
Hibernate	Hibernate is an object-relational mapping (ORM) solution for the Java language, and provides an easy to use framework for mapping an object-oriented domain model to a traditional relational database. Its purpose is to relieve the developer from a significant amount of relational data persistence-related programming tasks. See http://www.hibernate.org/ for more information.
IDP	Identity Provider. Is also sometimes shown as "IdP". For more information, see http://asc.gsa.gov/portal/template/faq08.vm .
JAR	JAR file is a file format based on the popular ZIP file format and is used for aggregating many files into one. A JAR file is essentially a zip file that contains an optional META-INF directory.
JAAS	The JAAS 1.0 API consists of a set of Java packages designed for user authentication and authorization. It implements a Java version of the standard Pluggable Authentication Module (PAM) framework and compatibly extends the Java 2 Platform's access control architecture to support user-based authorization.
SAML	Security Assertion Markup Language (SAML) is an XML standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee
Spring	Spring Framework is a leading full-stack Java/JEE application framework. Led and sustained by Interface21, Spring delivers significant benefits for many projects, increasing development productivity and runtime performance while improving test coverage and application quality. See http://www.springframework.org/ for more information.

Term	Definition
WSDD	An acronym for Web Service Deployment Descriptor, which can be used to specify resources that should be exposed as Web Services. See http://ws.apache.org/axis/java/user-guide.html#CustomDeploymentIntroducingWSDD for more information.
WSDL	An acronym for Web Services Definition Language, which is an XML-based language that provides a model for describing Web services. See http://www.w3.org/TR/wsdl.html or http://en.wikipedia.org/wiki/WSDL for more information.
XSD	XML Schema Definition.

Index

A

API

- authenticating users, 17
 - CGMM, 7, 11
 - CGMM Manager, 12
 - configuration files, 18
 - importing authentication, 16
 - importing CGMM Manager, 16
 - migrating users, 17
 - obtaining authentication, 17
 - obtaining CGMM Manager, 17
 - services, 12
 - workflow, 11
- authenticating users, 17
- authentication, 6

B

- before you install, 35

C

- caGrid account
- create new, 7, 25
- caGrid security infrastructure, 35
- CGMM
- API, 7, 11
 - API configuration, 18
 - API services, 12
 - architecture, 6
 - components, 7
 - customization, 7
 - deployment, 33, 36, 37
 - filter, 7
 - installation, 33, 34
 - installation parameters, 36
 - overview, 5
 - process flow, 7
 - release contents, 34
 - security concepts, 8
- CGMM Manager class, 12
- CGMM Properties sample file, 45
- CGMM Properties XSD file, 41
- CGMM Tool, 21
- customizing, 32
 - overview, 7
 - workflow, 21
- configuration files, 18
- create caGrid account, 7, 25
- create CSM account, 31
- customize CGMM Tool, 32

D

- deploying CGMM, 33, 36, 37
- Dorian, 8

F

- filter intercept, 7

G

- GAARDS
- authentication, 5
 - components used, 6
- Glossary, 53
- grid trust fabric
- synching, 18

H

- host application
- authentication, 6
 - environment requirements, 36
 - installation pre-requisites, 35
 - integrating with API, 16
 - issues solved, 6
 - login after migration, 25, 28
 - migration filter, 6
 - refactoring, 35
- HTTP filter, 7

I

- identity provider, 8
- importing authentication API, 16
- installing CGMM, 33, 34
- integrating the API, 11, 16

J

- JAAS deployment, 38
- JBoss deployment, 38, 39

M

- migrate
- CSM account, 24, 28
 - to existing Grid account, 30
 - to new Grid account, 27
 - without CSM account, 31
- migrating users, 17
- migration process, 6, 21
- minimum requirements, 9

O

- obtaining authentication API, 17
- overview
 - CGMM, 5
 - CGMM Tool, 7, 21
 - configuration files, 18

R

- related documents, 2
- release contents, 34
- release schedule, 4

S

- sample Sync description file, 47
- security caGrid infrastructure, 35
- security concepts, 8
- submit support issue, 4

- SyncGTS, 8, 32
- SyncGTS servlet, 11, 18
- synching with trust fabric, 18

U

- user login
 - after migration, 25, 28
 - caGrid account, 28
 - CSM account, 22, 25
- user migration process, 21
- user provisioning, 5
- using caGrid login, 23, 28
- using CSM login, 22, 25

W

- workflow for API integration, 11
- workflow for CGMM tool, 21