Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
# Table of Contents

1. **Security Overview** ............................................................................................................. 1  
   Oracle Software Security Assurance .................................................................................. 1  
   Secure Configuration Initiative ......................................................................................... 1  
   The Security Guides Program .......................................................................................... 1  
   Other Resources ............................................................................................................... 1  

2. **Secure Configuration** .................................................................................................... 3  
   Securing RMI Communications ......................................................................................... 3  
   Enabling SSL on Oracle ATG Web Commerce Service Center Applications .................. 4  
   Guarding Against Attacks through Request-Handling Pipeline Configuration ............... 4  
   Customizing a Request-Handling Pipeline ...................................................................... 5  
   Setting Access Levels for Properties Files ...................................................................... 5  
   Encrypting Credit Card Numbers in CRS ........................................................................ 5  
   Hashing Passwords in LDAP Profile Repositories ........................................................... 6  
   Securing LDAP Repositories ............................................................................................ 7  
   InitialContextEnvironment ............................................................................................... 7  
   Password Hashing ............................................................................................................ 8  
   Encrypted Properties in Nucleus Components ................................................................ 8  

3. **Security Features** ........................................................................................................... 9  
   Configuring and Using Authentication ............................................................................ 9  
   Configuring Security Related to User Profiles .............................................................. 9  
   Customizing Portal Authentication ............................................................................... 9  
   Configuring Authentication for the ATG Dynamo Server Admin ................................... 9  
   Configuring the Request-Handling Pipeline to Manage Authentication ...................... 10  
   CSC Agent Authentication for Live Help On Demand Click-to-Call ............................ 10  
   Authentication for REST Web Services .......................................................................... 10  
   Configuring and Using Access Control ......................................................................... 10  
   Core Access-Control Facilities for Users, Groups, Roles, Privileges, and Access Control Lists (ACLs) ......................................................................................................................... 10  
   Configuring Access Control for Secured Repositories .................................................. 11  
   Configuring Access Control for Assets, Projects, and Workflows in Content Administration .................................................. 11  
   Configuring Access Control for ATG Commerce Service Center Agents .................. 11  
   Configuring Access Control for the Business Control Center ..................................... 11  
   Creating Organizations and Roles ................................................................................ 11  
   Configuring Users and Roles in Merchandising ............................................................. 11  
   Configuring Access Control for Multisite Administration ............................................. 12  
   Using the Dynamo User Directory to Control Access to Organizations, Roles, and Principals .......................................................... 12  
   Setting up Access Control for Scenarios and Workflows ............................................... 12  
   Configuring Access Control for ATP Portal ................................................................. 12  
   Access control for SOAP and REST Web services ....................................................... 12  
   Access Control Servlet in CRS and CSC ........................................................................ 12  
   OrderLookup Servlet in Commerce .............................................................................. 13  
   Configuring and Using Security Audit ......................................................................... 13  
   Logging System Events and Collecting Data in ATG Portal ......................................... 13  
   Audit Logging of Actions by CSC agents ....................................................................... 13  
   Audit Trail for Pricing in CSC .......................................................................................... 13  
   Recording an Audit Trail for Scenario Activity ............................................................ 13  
   User Event Logging ........................................................................................................ 14  
   Content Event Logging ................................................................................................... 14  

Index ................................................................................................................................... 15
1 Security Overview

The chapter discusses the Oracle software security assurance initiative and how it relates to the Oracle ATG Web Commerce Suite.

Oracle Software Security Assurance

Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle’s methodology for building security into the design, build, testing, and maintenance of its products. Oracle’s goal is to ensure that Oracle’s products, as well as the customer systems that leverage those products, remain as secure as possible.

Secure Configuration Initiative

Part of this effort is the Secure Configuration Initiative program which ensures that the Oracle products install, out of the box, into a secure state. For more information on the goals of this initiative, see http://www.oracle.com/us/support/assurance/initiative/index.html.

The Security Guides Program

The Secure Configuration Initiative program also includes the Security Guides program which ensures that all Oracle products have a comprehensive documentation on configuring and using the products securely.

The ATG Commerce Security Guide

Details about security in the ATG Commerce Suite are discussed throughout the Oracle ATG Web Commerce Suite documentation set. This guide is intended to provide a high-level discussion of security in the Oracle ATG Web Commerce Suite with links to details in those various documents.

Other Resources

Developers producing customer-facing Web sites using the ATG Commerce Suite can make use of the security features of the platform. For other insights into secure coding practices and other general methods for making your web sites secure, consider using information provided by the Open Web Application Security Project (OWASP), see www.owasp.org.
This chapter discusses security considerations for immediate post-installation configuration of Oracle ATG Web Commerce. It particularly concentrates on login, SSL, and inter-application communication issues. These considerations are largely invisible to end users, but are critical for application security.

Each section in this chapter provides a brief overview of the security issue under consideration, and provides pointers for more detailed information regarding that issue.

This chapter includes the following sections:

- Securing RMI Communications (page 3)
- Enabling SSL on Oracle ATG Web Commerce Service Center Applications (page 4)
- Guarding Against Attacks through Request-Handling Pipeline Configuration (page 4)
- Setting Access Levels for Properties Files (page 5)
- Encrypting Credit Card Numbers in CRS (page 5)
- Hashing Passwords in LDAP Profile Repositories (page 6)
- Securing LDAP Repositories (page 7)
- Encrypted Properties in Nucleus Components (page 8)

## Securing RMI Communications

Oracle ATG Web Commerce servers can expose certain components to other applications through Java remote method invocation (RMI). To use this feature, you must first write a service according to the RMI specifications, then register your service with the Oracle ATG Web Commerce RMI server. After registering, other applications can access the service. It is important to insure that these applications access your service in a secure manner.

For more information, see the *ATG Platform Programming Guide*.

You can secure RMI communications by transmitting them over SSL. (For information on non-SSL RMI service implementations, the *ATG Platform Programming Guide*.)

### Configuring Keys and Certificates

To use RMI over SSL, configure both public and private keys and wrap the public key in a self-signed certificate. In a production environment, you must create a key store, trust store, and certificate, as described in the *Generating a New Certificate* section of the *ATG Platform Programming Guide*.
For more information about SSL keys and certificates, and for documentation about the Java Secure Socket Extension (JSSE) APIs, see the Oracle Web site.

Enabling SSL on Oracle ATG Web Commerce Service Center Applications

Secure Sockets Layer (SSL) is a cryptographic protocol that provides communication security over the Internet. SSL encrypts the segments of network connections at the Application Layer for the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity.

Commerce Service Center applications use SSL during user log-in. When using HTTPS, you must disable the default access controller. The <ATG10dir>/Service10.2/Service/Framework/Agent/liveconfig/atg/userprofiling/ProtocolAccessController.properties file identifies a number of settings required when using HTTPS.

For more detail, see Configure SSL in the ATG Installation and Configuration Guide.

Guarding Against Attacks through Request-Handling Pipeline Configuration

One of the most important tasks for an Oracle ATG Web Commerce server is handling HTTP requests. The request-handling pipeline represents a potential source of security issues related to denial of service attacks, and configuration should be approached carefully.

The Oracle ATG Web Commerce server extends the basic web server model with Nucleus services that implement the Servlet interface, and which are linked in order to process HTTP requests. Each servlet performs a specialized function on a request, then relays the request—sometimes in modified form—to the next servlet in the chain. While each servlet performs a unique service, it often relies on changes that previous servlets made to the request. This chain of servlets is called a request-handling pipeline.

For example, a typical request might be processed as follows:

1. Compare the request URI against a list of restricted directories, to make sure that the user has permission to access the specified directory.
2. Translate the request URI into a real file name, taking index files into account when the file name refers to a directory.
3. Given the file name’s extension, determine the MIME type of the file.
4. From the MIME type, dispatch the request to the appropriate handler.

The preceding example shows one of many request-handling configurations. Other configurations might dispatch based on a beginning path such as /cgi-bin or move the session-tracking step to be performed only for files with the MIME type text/session-tracked.
Because the request-handling pipeline is composed of Nucleus components that are independently configurable, it is easy to modify, giving you the flexibility that enterprise applications often require. For additional information on pipeline configuration, see the ATG Platform Programming Guide.

Customizing a Request-Handling Pipeline

The ATG installation provides a servlet pipeline that is invoked each time an ATG server handles a request. Dynamo Server Admin also has its own servlet pipeline, which starts with the servlet /atg/dynamo/servlet/adminpipeline/AdminHandler. You can construct pipelines used by your own applications, or you can customize existing ATG server pipelines.

For more information, see the Customizing a Request-Handling Pipeline section of the ATG Platform Programming Guide.

Basic HTTP Authentication

The BasicAuthenticationPipelineServlet class provides authentication using the Basic HTTP authentication mechanism. A component for this servlet is not included in the standard servlet pipelines, but the class is available for use in servlet pipelines you might create in your own applications. For enhanced security, it is recommended that you use a secure HTTPS protocol.

For more information see Authentication in the ATG Platform Programming Guide.

Browser Caching of Dynamic Pages

Some browsers handle page caching in a way that conflicts with dynamic page requests. ATG’s browser typer marks page requests from those browsers as non-cacheable to override the aggressive caching behavior of some browsers and proxy servers. This approach also helps avoid security exposure caused by proxy servers caching.

For more information on preventing browsers from caching dynamic pages, see the BrowserTyper section of the ATG Platform Programming Guide.

Setting Access Levels for Properties Files

ATG components are configured with plain text properties files. You should set access levels on your properties files so they cannot be altered or viewed by unauthorized users. Only site administrators should have read and write permissions. ATG must be invoked from an account with these permissions as well. The properties files that contain sensitive information typically reside in each server’s localconfig directory, but as a general practice, all ATG components should be secured.

For more information, see the Setting Access Levels for Properties Files section of the ATG Installation and Configuration Guide.

Encrypting Credit Card Numbers in CRS

By default, Oracle ATG Web Commerce does not apply any encryption to credit card information.
For more information on encrypting credit card information, see the Extensions to the credit-card Item Descriptor section of the ATG Commerce Reference Store Overview.

**Hashing Passwords in LDAP Profile Repositories**

Lightweight Directory Access Protocol (LDAP) directories are widely used to store personnel information and other kinds of data. ATG's LDAP profile repository is an implementation of the Repository API that enables you to store and access profile data in an LDAP directory.

By default, the Personalization module is configured to use a SQL profile repository, but you can change the configuration to use an LDAP repository instead. Using an LDAP repository enables you to tap into the profile data you already have in an LDAP directory, and to share user information across multiple applications.

Just like the SQL profile repository, the LDAP repository implements the ATG repository API to allow you to store, access, modify, and query user profile information. As in the SQL profile repository, repository items are first created as transient items (RAM profiles); they become persistent after they are added to the database.

For complete information about LDAP repository concepts, architecture, and code, see the LDAP Repositories chapter in the ATG Repository Guide.

It is important to note, however, that the LDAP repository implementation is not specific to user profiles in any way. Since an LDAP directory can be used to store any kind of data (people, groups, mailing lists, documents, printers, etc.), you could use the LDAP repository to expose any of that data in an ATG application.

For more information, refer to the LDAP Repositories chapter in the ATG Repository Guide.

**Scenarios module and LDAP Repositories:** You cannot use scenarios with an LDAP profile repository, because the LDAP repository is not currently powerful enough to express all the data relationships required by the Scenarios module. If you want to run scenarios, you must use either a SQL repository or a composite repository to store all profile information.

**Creating the LDAP Profile Repository Component**

The LDAP profile repository is a component of class `atg.adapter.ldap.LDAPRepository`. Create and configure an instance of this component as described in the LDAP Repositories chapter of the ATG Repository Guide.

**Configuring the Personalization Module to use the LDAP Repository**

By default, the Personalization module is configured to use a SQL database to store profiles. To use an LDAP directory instead, you need to configure the following Personalization module components to work with the LDAP repository.

For more information, see the Configuring the Personalization Module to use the LDAP Repository section of the ATG Personalization Programming Guide.

**LDAP Password Encryption**

The `passwordHasher` property of the `atg/userprofiling/PropertyManager` component points to a password hasher component that handles password encryption.
For more information, see the LDAP Password Encryption section of the ATG Repository Guide.

For LDAP servers other than Oracle Directory Server, you may need to create your own PasswordHasher implementation, if none of the PasswordHasher implementations included in the ATG platform meet your requirements.

For more information, see the Password Hashing section in the Customizing Application Security chapter of the ATG Platform Programming Guide for more information about ATG’s PasswordHasher implementations.

For more information, see User Profiling Tools in the ATG Personalization Programming Guide.

**LDAP Profile Repository Definition File**

For a sample LDAP profile repository definition file, see the Sample LDAP Profile Repository Definition File section of the ATG Platform Programming Guide.

**Securing LDAP Repositories**

The Oracle ATG Web Commerce LDAP Repository is an implementation of the Repository API that enables you to store and access profile data in an LDAP (Lightweight Directory Access Protocol) directory. The LDAP repository is similar in functionality to the SQL repository, as described earlier in this guide. While by default Oracle ATG Web Commerce Scenario Personalization is configured to use an SQL profile repository, you can change the configuration to use an LDAP repository instead.

See the ATG Personalization Programming Guide for information about configuring Oracle ATG Web Commerce to use an LDAP profile repository. LDAP directories are widely used to store personnel information and other kinds of data. LDAP repository lets you to tap into the profile data you already have in an LDAP directory, and to share user information across multiple applications.

Also, you can configure Oracle ATG Web Commerce’s application security scheme to use an LDAP repository, rather than an SQL repository. See the Managing Access Control chapter in the ATG Platform Programming Guide for more information.

Just like the SQL repository, the LDAP repository implements the Oracle ATG Web Commerce Repository API to allow you to store, access, modify, and query user profile information. As in the SQL repository, repository items are first created as transient items (RAM profiles); they become persistent after they are added to the database.

It is important to note, however, that the LDAP repository implementation is not specific to user profiles in any way. Because an LDAP directory can be used to store any kind of data—people, groups, mailing lists, documents, printers—you can use the LDAP repository to expose any of that data in Oracle ATG Web Commerce.

See the ATG Platform Programming Guide for an introduction to LDAP terminology, architecture, and concepts.

**InitialContextEnvironment**

For details on the component that specifies the JNDI environment properties used to create a JNDI InitialDirContext to point to your LDAP directory server see the /atg/adapter/ldap/InitialContextEnvironment section of the ATG Repository Guide. You must configure this component to point to your LDAP directory server.
Password Hashing

The `passwordHasher` property of the `/atg/userprofiling/PropertyManager` component points to a password hasher component that handles password encoding.

For more information, see the LDAP Password Encryption section of the ATG Personalization Programming Guide.

For LDAP servers other than Oracle Directory Server, you might need to create your own `PasswordHasher` implementation, if none of the `PasswordHasher` implementations included in the Oracle ATG Web Commerce platform meet your requirements.

See the Working with User Profiles chapter of the ATG Personalization Programming Guide for more information about configuring the PropertyManager component.

For detail on password encoding and encryption for Web services, see the Web Services for Personalization and Scenarios sections of the ATG Personalization Programming Guide.

Encrypted Properties in Nucleus Components

You might decide to encrypt sensitive information that is stored in properties files with a symmetrical/asymmetrical encryption method. In this case, you must be able to access the encrypted information. A Base64 encoding method should not be used.

For more information, see the Decoding Encrypted Properties in Nucleus Components section of the ATG Platform Programming Guide.
3 Security Features

This chapter discusses key security features in the ATG Commerce Suite. These features include mechanisms for authentication, access control, and security audit.

The section below identifies places in the ATG Commerce Suite documentation that discuss these security features in more detail.

This chapter includes the following sections:
- Configuring and Using Authentication (page 9)
- Configuring and Using Access Control (page 10)
- Configuring and Using Security Audit (page 13)

Configuring and Using Authentication

These topics relate to configuration options involving user authentication.

Configuring Security Related to User Profiles

This area includes use of different authentication mechanisms, password expiration, password rule checks, password hashing, and securing cookies with hash keys.

For more information, see the ATG Personalization Programming Guide, Working with User Profiles.

Customizing Portal Authentication

ATG Portal features default user authentication pages, which you can customize (or replace with different ones). The default set of authentication pages includes login and logout forms, and an access denied page. The authentication configuration allows pages to be assigned on a device-specific and community-specific basis.

For more information, see the ATG Portal Development Guide, Customizing Portal Authentication.

Configuring Authentication for the ATG Dynamo Server Admin

By default, ATG Dynamo Server Admin requires password authentication to run.
For more information, see the ATG Platform Programming Guide, Developing and Assembling Nucleus-Based Applications.

Configuring the Request-Handling Pipeline to Manage Authentication

The BasicAuthenticationPipelineServlet class provides authentication using the Basic HTTP authentication mechanism.

For more information, see the ATG Platform Programming Guide, Request Handling with Servlet Pipelines, Request Handling Pipeline Servlets Reference.

CSC Agent Authentication for Live Help On Demand Click-to-Call

Live Help On Demand Click to Call is an optional application that, when integrated with Commerce Service Center, initiates and manages telephone communication between agents and customers. Commerce Service Center authenticates the data request and the agent user ID before transferring any data. Commerce Service Center authentication uses values that are calculated based on values in the request and a secret key value.

For more information, see the ATG Commerce Service Center Installation and Programming Guide.

Authentication for REST Web Services

Before you can use the Oracle ATG Web Commerce platform REST Web Services you must log in to open an authorized HTTP session. When the server receives a log in request for a valid user account, it will authenticate the user and return a session identifier if the authentication is successful.


Configuring and Using Access Control

These topics relate to configuration options involving user access control.

Core Access-Control Facilities for Users, Groups, Roles, Privileges, and Access Control Lists (ACLs)

User account security is managed through the atg.security API. Using this API, you can manage persistent user accounts, look up user identities and associate them with roles, manage access control lists, and tie together multiple security systems running against the same user account database and/or authentication mechanisms.

The Security Services Interface is a set of fast, flexible APIs that you can use in an application to provide security for the application’s features. The Security Management Interface enables programmers to configure account and privilege information with minimal programming.
For more information, see the ATG Platform Programming Guide, Managing Access Control.

### Configuring Access Control for Secured Repositories

The Oracle ATG Web Commerce secured repository system works in conjunction with the Oracle ATG Web Commerce Security System to provide fine-grained access control to repository item descriptors, individual repository items, and individual properties through Access Control List (ACL) settings.

For more information, see the ATG Repository Guide, Secured Repositories.

### Configuring Access Control for Assets, Projects, and Workflows in Content Administration

Access to assets, projects, and workflows in ATG Content Administration is highly configurable.

For more information, see the ATG Content Administration Programming Guide, Managing User Access and Security.

### Configuring Access Control for ATG Commerce Service Center Agents

When Commerce Service Center is installed, it is preconfigured with various access rights, global roles, and access controllers. These elements are used to restrict access to certain pages in Commerce Service Center.

For more information, see the ATG Commerce Service Center Installation and Programming Guide, Setting Up.

### Configuring Access Control for the Business Control Center

The Business Control Center provides various levels of security, which you can use to control access to the entire UI, to specific activities, or to assets managed within it.

For more information, see the ATG Business Control Center Administration and Development Guide, ATG Business Control Center Security.

### Creating Organizations and Roles

In addition to setting up profiles for individual users (customers who are site visitors, or other types of site users such as administrators), you can set up additional profiles for abstract entities called “organizations” and “roles” and use them to create a multi-level organization of site users grouped by function.

For more information, see the ATG Personalization Guide for Business Users, Setting Up Visitor Profiles.

### Configuring Users and Roles in Merchandising

Without modification after installation, user access to the Merchandising application is limited to an evaluation Content Administration publishing user account, the administrative user, and the Merchandising user who enables access to all non-administrative parts of the Business Control Center.

For more information, see the ATG Merchandising Administration Guide, Configuring Merchandising, the ATG Search Installation and Configuration Guide ATG Search Overview, and the ATG Search Administration Guide, Overview.
Configuring Access Control for Multisite Administration

Site Administration allows you to share data as well as configure and maintain the sharing relationships between sites. When working in a multisite environment, you can configure sites to share data. Data such as Nucleus components or data objects can be identified as shareable types. Site administrators combine shareable types and sites into a site group, where the shareable types are used by all sites in the group. Access to this data is controlled by managing roles using Site Administration in the Business Control Center.

See the ATG Multisite Administration Guide, Sharing Data.

Using the Dynamo User Directory to Control Access to Organizations, Roles, and Principals

The Dynamo User Directory allows you to assign access rights to repository items.

For more information, see the ATG Personalization Programming Guide, Working with the Dynamo User Directory.

Setting up Access Control for Scenarios and Workflows

You can grant or deny access to the features of the Scenarios module by displaying or hiding menu items in the main ACC window.

For more information, see the ATG Personalization Programming Guide, Setting Up and Setting Up Security Access for Workflows.

Configuring Access Control for ATP Portal

ATG Portal is subject to the security settings specified within the ATG platform. PAF security settings are handled primarily from the administrator interface, although additional tags and methods are available to further maintain portal security from within individual gears and the PAF itself.


Access control for SOAP and REST Web services

The Oracle ATG Web Commerce platform SOAP and REST Web Services use the underlying security system of the Oracle ATG Web Commerce platform.

For more information, see the ATG Web Services Guide.

Access Control Servlet in CRS and CSC

The Access Control Servlet can allow or deny access to a page or group of pages based on criteria such as membership in a group or satisfaction of a targeting rule.

For more information, see the ATG Commerce Service Center Installation and Programming Guide and the CRS-IUA Overview for more information.
OrderLookup Servlet in Commerce

The OrderLookup servlet bean retrieves one or more Order objects, depending on the supplied input parameters. OrderLookup has a security feature that allows the current user to view only her own orders. By default, this feature is enabled for /atg/commerce/order/OrderLookup. To disable the feature, set the enableSecurity property to false.

For more information, see the OrderLookup section of the ATG Commerce Guide to Setting Up a Store for more information.

Configuring and Using Security Audit

These topics relate to configuring and using security audit to bolster software security.

Logging System Events and Collecting Data in ATG Portal

Oracle ATG Web Commerce includes three different systems for sending, receiving, and recording messages generated by components: Logging, Data Collection, and Recorders. Oracle ATG Web Commerce Logging provides a convenient way to log system messages.

For more information, see the ATG Portal Development Guide, Logging and Data Collection.

Audit Logging of Actions by CSC agents

Commerce Service Center uses audit logging to record actions performed by Commerce Service Center agents in the agent audit repository.

For more information, see the ATG Commerce Service Center Installation and Programming Guide, Programming ATG Commerce Service Center.

Audit Trail for Pricing in CSC

Commerce Pricing Calculators provide options for audit trails which can be used for security related purposes.

For more information, see the ATG Commerce Service Center Installation and Programming Guide, Commerce Pricing Calculators.

Recording an Audit Trail for Scenario Activity

For the purposes of managing your company’s relationship with its site visitors, it is useful to be able to track what happens as a result of the elements within a scenario. For example, if you set up a scenario that sends a promotional e-mail to new members offering them a discount on a product, it is helpful to keep a record of the members to whom the e-mail is sent. Information such as this can help you monitor the success of your promotions, and it also allows you to provide better customer service.

For more information, see the ATG Personalization Guide for Business Users, Creating Scenarios and the ATG Personalization Programming Guide.
User Event Logging

When you send events to the ATG logging system, you can record useful information about the operation of your Web application. The Personalization module’s logging system handles page requests (from URLs), user events (such as new session, login, etc), and content viewed from Content Repositories.

For more information, see the ATG Personalization Programming Guide, Personalization Module Logging.

Content Event Logging

ATG Personalization lets you customize content for specific users and events, including event logging.

For more information, see the ATG Page Developer’s Guide, Serving Targeted Content with ATG Servlet Beans.
Index

A
access levels
  properties files, 5

B
Base64 encoding, 8
BasicAuthenticationPipelineServlet, 5
browser
  caching behavior, 5

D
DAS servlet pipeline
  BasicAuthenticationPipelineServlet, 5
definition file
  LDAP repository, 7

E
encryption, 8

H
HTTP request handling pipeline, 4
  custom components, 5
HTTPS, 4

J
Java remote method invocation (see remote method invocation (RMI))

L
LDAP (Lightweight Directory Access Protocol), 7
LDAP profile repository, 6
  and Scenarios module, 6
  component, 6
  configuring Personalization module components, 6
  definition file, 7
  password encryption, 6
LDAP repositories, 7
LDAP repository
  password encryption, 8

Lightweight Directory Access Protocol (see LDAP) (see LDAP (Lightweight Directory Access Protocol))

N
Nucleus component properties
  encrypted, 8

P
password encryption
  LDAP repository, 8
password hashing (see password encryption)
passwords
  encrypting in LDAP repositories, 6
  hashing, 6
  properties files, 5
profile repository
  LDAP (see LDAP profile repository)
ProfileTools component
  configuring, for LDAP profile repository, 6
  properties files
  setting access levels, 5
PropertyManager component
  configuring, for LDAP profile repository, 6
PropertyValueDecoder, 8

R
remote method invocation (RMI), 3
repositories
  LDAP (see LDAP repositories)
repository definition file
  LDAP, 7
request handling (see HTTP request handling)
RMI (see remote method invocation (RMI))
RmiServer, 3, 3
  (see also remote method invocation (RMI))

S
scenarios
  LDAP repositories, 6
  running against an LDAP repository, 6
servet pipeline
  BasicAuthenticationPipelineServlet, 5
HTTP request handling, 4
SSL, 4
  keys and certificates, 3