HP ALM

Software Version: 12.00

Secured Deployment and Configuration Guide

Document Release Date: March 2014

Software Release Date: March 2014

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Intel® is a trademark of Intel Corporation in the U.S. and other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
  - The number before the period identifies the major release number.
  - The first number after the period identifies the minor release number.
  - The second number after the period represents the minor-minor release number.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition, visit the following URL:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the New users - please register link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP Software support web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require an active support contract. To find more information about support access levels, go to the following URL:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to the following URL:

http://h20229.www2.hp.com/passport-registration.html

Contents

Welcome to This Guide

Introduction

Welcome to the HP ALM Secured Deployment and Configuration Guide.

This guide is designed to help IT professionals who deploy and manage Application Lifecycle Management (ALM) instances in a secure manner in the modern enterprise. Our objective is to help you make well-informed decisions about the various capabilities and features that ALM provides to meet modern enterprise security needs.

Security requirements for the enterprise are constantly evolving and this guide should be viewed as HP's best effort to meet those stringent requirements. If there are additional security requirements that are not covered by this guide, please open a support case with the HP support team to document them and we will include them in future editions of this guide.

1 Secure Implementation and Deployment

This chapter provides information on implementing and deploying ALM in a secure manner.

Technical System Landscape

ALM is an enterprise-wide application based on Java 2 Enterprise Edition (J2EE) technology. J2EE technology provides a component-based approach to the design, development, assembly, and deployment of enterprise applications. For details, see the *About ALM Technology and Architecture* section of the *ALM Installation and Upgrade Guide*.

Security in Basic ALM Configuration

For security recommendations for a basic ALM Configuration, see the *Example of Basic ALM Configuration* section of the *ALM Installation and Upgrade Guide*.

Security in Clustered ALM Configuration

For security recommendations for a clustered ALM Configuration, see the *Example of Clustered ALM Configuration* section of the *ALM Installation and Upgrade Guide*.

External Authentication

ALM supports external authentication with specific configurations. The supported modes include Smart Card authentication, such as CAC, and SSO authentication, such as Siteminder. For details, see the *ALM External Authentication Configuration Guide*.

Proxy Authentication Support

When a proxy or front end web server requires authentication, you can use the Webgate Customization tool to configure the proxy and identify the credentials it expects, as well as any required front end web server credentials. For more information, see the *HP ALM Webgate Customization Readme*, available from **Help > ALM Tools > Webgate Customization**.

Common Security Considerations

Thoroughly review the trust boundaries between ALM components (ALM servers, Performance Center servers, exchange servers, database servers, LDAP servers, and other integrating servers) to minimize the number of hops between the components. In addition, it is recommended to use SSL to secure access to servers located across such boundaries.

Note: Currently, a secure channel to the database server from ALM is not supported.

When there is a firewall between any ALM deployment components, ensure the proper configuration according to the vendor recommendation.

Run periodic trusted root Certificate Authority certificate updates on your clients and servers to ensure that the publisher certificates used in digital code signing are trusted.

Best Practice

The ALM application server does not have SSL enabled. It is expected and recommended that the front end server, either the load balancer or the reverse proxy will be configured to require SSL.

2 ALM Security Site Settings

This chapter contains reference to some of the ALM site parameters that are relevant to security. Full details can be found in the *ALM Administration Guide*.

Secure ALM Storage

ALM allows users to upload files to the server. This allows users to upload attachments, save automation scripts and test run results, and so on. All files uploaded to the server must be validated, since they can contain viruses, malicious code, or Trojan horses that could infect the entire system. An attacker or a malicious user can upload malicious files from one account and then download them to diverse clients.

The site administrator can limit the types of files that can be uploaded to ALM by using the **FILE_EXTENSION_BLACK_LIST_UPLOAD** site parameter, which filters unwanted file types by extension. However, the attachment files can contain dangerous content. As a result, a downloaded file must still be opened with caution.

It is strongly recommended to implement proper antivirus protection for the file storage allocated for the ALM repository.

The site administrator can restrict the download of specific file types as described below.

In addition, the size of the file uploaded as an attachment can be limited by setting the **UPLOAD_ATTACH_MAX_SIZE** site parameter.

Since ALM provides an OTA API to work with file storage, it is recommended to secure the API by setting the **DISABLE_EXTENDED_STORAGE** and **RESTRICT_SERVER_FOLDERS** site parameters.

Secure ALM Client Installation

As mentioned above, attachment files can contain dangerous content. As a result, a downloaded file must be opened with caution. The site administrator can help protect the ALM client by using the **FILE_EXTENSION_BLACK_LIST_DOWNLOAD** and **DOWNLOAD_REST_ATTACHMENTS** site parameters to restrict certain file types from being downloaded to the client machine.

Secure Access to Excel Report Query Execution

Business View Microsoft Excel reports use DQL queries to retrieve data from the database. The user cannot manually edit SQL queries generated from DQL to insert forbidden commands.

For DQL limitations, see the *Working with DQL* section of the *ALM Administrator Guide*. You can customize the maximum number of records that can be retrieved from the database by setting Row Limit in Excel. For details, see the *ALM Business Views Microsoft Excel Add-in User Guide*.

Secure Debug Features

ALM provides a set of tools for troubleshooting and to provide better supportability. These features, which can expose sensitive internal information about the system and about activities performed on the system, are disabled by default and can be switched on by using the following site parameters. It is recommended to validate that the parameters are reset to the default values immediately after using the debug feature.

The debug related site parameters are:

- **ENABLE_JMX_CONSOLE**
- **ENABLE_PERFORMANCE_MONITOR_BIRT_REPORTS**
- **DISABLE_CONSOLE_DEBUG_INFO**
- **DISABLE_COMMAND_INTERFACE**
- **DISABLE_VERBOSE_ERROR_MESSAGES**

Secure Access to ALM

- Display of the last user login name is controlled by the **DISPLAY_LAST_USER_INFO** site parameter.
- Whether a project administrator can change user details is controlled by the **ALLOW_UPDATE_USER_PROPERTIES _FROM_CUSTOMIZATION** site parameter.
- Whether users can reset their passwords using the Forgot Password link is controlled by the **PASSWORD_RESET_DISABLE**, **PASSWORD_RESET_VALID_PERIOD**, and **PASSWORD_RESET_SERVER** site parameters.
- Whether to restrict SSL communication to the login process only is controlled by the **FORCE_LOGIN_SSL_MODE** site parameter. For more information, see *http://support.openview.hp.com/selfsolve/document/KM00756801*.
- The following site parameters control the user session:
    - **WAIT_BEFORE_DISCONNECT**
    - **FAST_RECONNECT_MODE**
    - **AUTO_LOGOUT_ON_SERVER_DISCONNECT**

Best Practice

Set the **UPLOAD_ATTACH_MAX_SIZE** site parameter to limit the size of the file uploaded as an attachment.

3 Installation Security

This chapter provides information on aspects of installation security.

Supported Operating Systems

For the list of supported system environments, see the *Readme*.

Note: The supported environment information in the *Readme* is accurate for the ALM12.00 release, but there may be subsequent updates. For the most up-to-date supported environments, see the HP Software Web site using the following URL: *http://www.hp.com/go/TDQC_SysReq*.

Web Server Security Recommendations

IIS Web Server

See *http://www.iis.net/* for information on enabling SSL for all interactions with the web server.

Note: SSL should be enabled for the entire IIS web server under which you installed the ALM applications.

To disable weak ciphers on IIS, see *http://support.microsoft.com/kb/187498/en-us*.

Apache Web Server

See *http://httpd.apache.org/docs/current/ssl/ssl_howto.html* for information on enabling SSL for all interactions with the web server and on enforcing strong security.

Application Server Security Recommendations

- When configuring SSL on the ALM application server, keep your keystore in a private directory with restricted access. Although the Java keystore is password protected, it is vulnerable as long as the password was not changed from its default value of *changeit*.
- Always change default passwords.
- Always obfuscate passwords entered into the jetty.xml file. For more information, see *http://www.eclipse.org/jetty/documentation/current/configuring-security-secure-passwords.html*.
- Since the default *td* user password is documented in ALM, it is strongly recommended to change the *td* user's password. This is done during the installation in the *Create new SA schema* step, if the *td* user does not yet exist in this database server. Each subsequent installation that uses the same database server uses the existing *td* user credentials. To change the password for the previously created *td* user, follow the steps in *http://support.openview.hp.com/selfsolve/document/KM773656*.
- Always change the default password when creating a database schema.
- Always use the minimal possible permissions when installing and running ALM.

Action	**Permissions Needed for User**
Installing ALM	• Windows: Administrator permissions • Linux: You can install with non -root permissions using the sudo command. For details, see the *ALM Installation and Upgrade Guide*.
Running ALM	• Windows: Windows service runs as the system user or a specific user (the user must have access to the file repository). • See the *ALM Installation and Upgrade Guide* for the set of required permissions..

Database connection	The *td* user permissions must be set properly according to the recommendations in the *ALM Installation and Upgrade Guide*. Do not use a higher level of permissions than required. Do not use the default password when creating the schema.

FAQ

Question

Does ALM ensure that configuration files are not stored in the same directory as user data?

Answer

The user can change the location of the repository and log files according to best practices to avoid mixing user data with configuration files.

Question

Does ALM install with unnecessary functionality disabled by default?

Answer

Yes, functionality is license driven.

Question

Are application resources protected with permission sets that allow only an application administrator to modify application resource configuration files?

Answer

Yes, only the user with permission to access specific directories on the ALM server machine can modify ALM configuration files.

Question

Does ALM execute with no more privileges than necessary for proper operation?

Answer

Yes, the permissions model is constantly reviewed and only necessary permissions are required. For permission details see the *ALM Installation and Upgrade Guide*.

4 Network and Communication Security

This chapter provides information on network and communication security.

Secure Topology

The ALM platform is designed to be part of a secure architecture, and can meet the challenge of dealing with the security threats to which it could potentially be exposed.

Several measures are recommended to securely deploy ALM servers:

- Reverse proxy architecture

  One of the more secure recommended solutions is to deploy ALM using a reverse proxy. ALM fully supports reverse proxy architecture as well as secure reverse proxy architecture. See the *ALM Installation and Upgrade Guide* for information on configuring a reverse proxy for ALM.

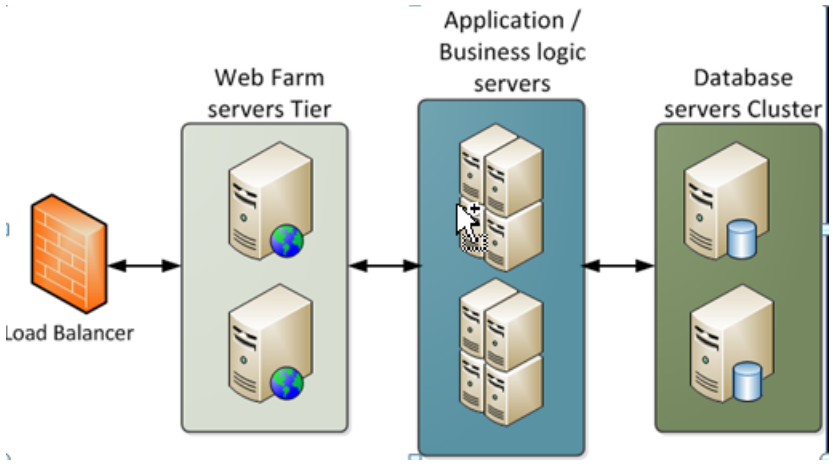
- SSL communication protocol

  The SSL protocol secures the connection between the client and the server. URLs that require a secure connection start with HTTPS instead of HTTP. ALM supports SSLv3 and TLSv1.

- DMZ architecture using a firewall

  The secure architecture referred to in this document is a typical DMZ architecture using a device as a firewall. The basic concept is to create a complete separation, and to avoid direct access, between the ALM clients and the ALM servers. This is especially important when opening access to ALM to external clients from outside of your organization.

- Separation between web servers, application servers, load balancers, and database servers



Reverse Proxy Overview

A reverse proxy is an intermediate server that is positioned between the client machine and the web servers. To the client machine, the reverse proxy seems like a standard web server that serves the client machine's HTTP or HTTPS protocol requests, with no dedicated client configuration required.

The client machine sends ordinary requests for web content, using the name of the reverse proxy instead of the name of a web server. The reverse proxy then sends the request to one of the web servers. Although the response is sent back to the client machine by the web server through the reverse proxy, it appears to the client machine as if it is being sent by the reverse proxy.

Reverse Proxy Security

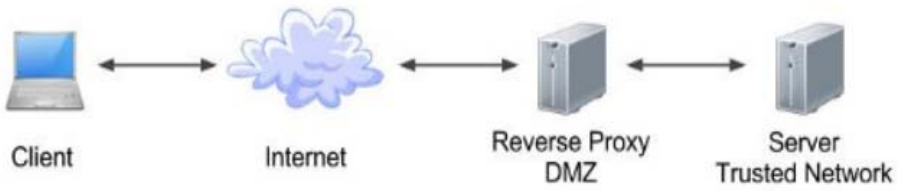
A reverse proxy functions as a bastion host. It is configured as the only machine to be addressed directly by external clients, and thus obscures the rest of the internal network. Use of a reverse proxy enables the application server to be placed on a separate machine in the internal network, which is a significant security objective.

DMZ is a network architecture in which an additional network is implemented, enabling you to isolate the internal network from the external one. Although there are a few common implementations of DMZs, this

chapter discusses the use of a DMZ and reverse proxy in a back-to-back topology environment.

The following are the main security advantages of using a reverse proxy in such an environment:

- No DMZ protocol translation occurs. The incoming protocol and outgoing protocol are identical (only a header change occurs).
- Only HTTP or HTTPS access to the reverse proxy is allowed, which means that stateful packet inspection firewalls can better protect the communication.
- A static, restricted set of redirect requests can be defined on the reverse proxy.
- Most of the web server security features are available on the reverse proxy (authentication methods, encryption, and more).
- The reverse proxy screens the IP addresses of the real servers as well as the architecture of the internal network.
- The only accessible client of the web server is the reverse proxy.
- This configuration supports NAT firewalls.
- The reverse proxy requires a minimal number of open ports in the firewall.
- The reverse proxy provides good performance compared to other bastion solutions.
- Using a secure reverse proxy architecture is easier to maintain. You can add patches to your reverse proxy as needed



Note:

- The ALM application server does not have SSL enabled. It is expected and recommended that the front end server (load balancer or reverse proxy) will be configured to require SSL.

- Follow security guidelines for LDAP servers and Oracle or SQL databases.
- Run SNMP and SMTP servers with low permissions.

Communication Channels Security

ALM supports the following secure channels:

Secure Channel	How to Configure
Between client (including testing tools) and ALM server	• In general, trust is only needed on the client. This is a trust to the authority that issued the server certificate for the ALM server. • If client certificate or smart card authentication is required, and there is no access to the internet, an offline OCSP (cache) server or local CRL should be used for the certificate revocation list (CRL). Otherwise, it can take a long time to log in to ALM due to timeouts in checking the online CRL. • There is a flag for debugging such situations that can be provided as a URL parameter, *cancelcrlcheck=true*. Providing this flag cancels the CRL check, and thus can determine if there is a CRL related issue • Use the Webgate Customization tool if proxy authentication is required.
Between ALM and LDAP server	For details, see the *Enabling LDAP over SSL* section of the *ALM Administration Guide*.
Between ALM and mail server	Specify a secure port when defining the mail server,
Between RP/LB and ALM server	Configure the ALM server with SSL (for details, see the *Configuring Secure Access* sections of the *ALM Installation and Upgrade Guide*). On the reverse proxy or load balancer, use a secure connection to the ALM server (for example, https://<almserver>:8443/qcbin)

FAQ

Question

Are exceptions required to be added to the firewall policy?

Answer

Placing a reverse proxy in front of the ALM server is recommended. The list of ports to be open in the firewall for the incoming traffic is documented in the *ALM Installation and Upgrade Guide* and in the *Performance Center Installation Guide*. The only port that must be opened on the ALM server for incoming traffic is the jetty port (8080, or 8443 if you are using a secure connection).

Question

How do I configure the ALM server in SSL using the certificate authority?

Answer

For details, see
http://support.openview.hp.com/selfsolve/document/KM00756782.

5 Site Administration Interface

This chapter provides information related to securing ALM Site Administration.

Access to Site Administration

To disable access to the site administration interface (not including project customization) from the outside, the following URIs can be blocked at the front end (either the load balancer or the reverse proxy):

- /qcbin/SiteAdmin.jsp
- /qcbin/addins.html
- /qcbin/servlet/tdsiteadminservlet/*
- /qcbin/debug/*

These URIs are subject to change and must be reviewed for each new major version of ALM.

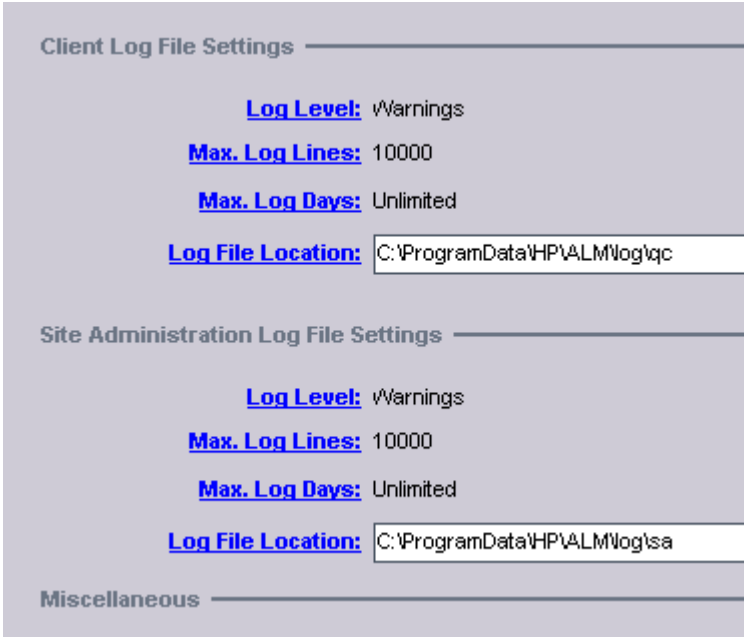
Access to project customization can be restricted at the permissions level.

To secure the site administration interface:

1. Change the site administrator password during the initial setup.
2. Use a strong password for the site administrator.

Site Administration Actions

Action	How to Access
Site admin	Log in to Site Administration via https://<server>/qcbin/SiteAdmin.jsp

Project admin	Log in to ALM through the desktop client as a project administrator.
Debugging user actions	1. Log in to Site Administration. 2. Open the **Servers** tab. 3. Select your server. 4. For client actions recorded on the server, use the **Client Log File Settings**. 5. For site administration actions, use the **Site Administration Log File Settings**. 6. Set the **Log Level** to debug.  **Note:** Make sure to turn off the debug when you are done.
Debugging	The debug console and QCSense reports are by default disabled (see the **DISABLE_CONSOLE_DEBUG_INFO** site parameter) since these features are for debug purposes and should be switched off immediately after debugging is finished.
Debugging	The **DISABLE_CONSOLE_DEBUG_INFO** site parameter controls access to the ALM debug info console page.

Debugging	The **ENABLE_JMX_CONSOLE** site parameter enables the JMX Console for debugging purposes.
Debugging	The **ENABLE_PERFORMANCE_MONITOR_BIRT_REPORTS** site parameter allows you to generate QC Sense reports for debugging purposes.
Debugging	The **DUMP_REQUEST_HEADERS** site parameter enables you to view request headers in the logs. This is helpful when you are configuring external authentication and are looking for the correct header that contains the user ID. To view this information, you must also set the site administration or client **Log Level** to debug.

Note: All debug features should be used for debug purposes only and should be switched off immediately after debugging is finished.

6 User Management and Authentication

This chapter provides information related to user authentication.

Authentication Model

ALM supports the following authentication methods:

- Form login
- External authentication
    - IDM-SSO (Siteminder) - with special configuration required
    - Smart Card - with special configuration required
    - Active Directory or any LDAP provider supporting the LDAP3 protocol

Authentication Administration and Configurations

Authentication is configured using Site Administration. For details, see the *Managing ALM Users* chapter of the *ALM Administration Guide*.

Following are additional references:

Action	**Reference**
Create and manage users using OTA API	*ALM Open Test Architecture API Reference*
Manage users using REST API	*ALM REST API Reference (Technical Preview)*
External authentication (Smart Card or SSO)	*ALM External Authentication Configuration Guide*

FAQ

Question

Can ALM require account passwords that conform to corporate policy?

Answer

LDAP integration is a recommended solution to ensure password policy support.

Question

Which LDAP providers does ALM support?

Answer

ALM works with any LDAP provider supporting the LDAP3 protocol.

Question

Describe the session management and session lockout mechanisms (that is, how does ALM verify the user's session, how does ALM respond if verification fails, is there a lockout time-out or can it be configured).

Answer

ALM manages user sessions on the application level. The session can be terminated by the site administrator at any time. All currently opened sessions can be viewed from the Site Administration console. Each session has an expiration time that can be configured by the **WAIT_BEFORE_DISCONNECT** site parameter for OTA APIs and the **REST_SESSION_MAX_IDLE_TIME** site parameter for REST APIs.

Question

Can ALM limit the number of logon sessions per user and per application?

Answer

Since ALM provides the possibility to connect from different interfaces, such as testing tools, UI, or API, there is no limit on the number of user logon sessions.

7 Authorization

This chapter provides information related to user authorization in ALM.

Authorization Administration

User access to ALM resources is authorized based on the user's role and group membership. See the *Managing User Groups and Permissions* chapter of the *ALM Administration Guide* for details.

By default, the user is assigned to each project as Viewer. However, the user can be assigned to specific user groups. The same groups can exist in different projects. The membership in these user groups is per project.

The same user assigned to multiple groups receives the highest permissions. When a user belongs to multiple groups, data hiding can be affected. Check the permissions across all groups.

It is recommended to use minimal permissions when creating new groups. Make sure to select appropriate role and base permissions for the group.. It is always recommended to grant minimal permissions and extend the permissions only as needed to avoid unwanted privilege escalation. For example, start with Viewer permissions and add additional permissions individually as needed.

FAQ

Question

Can ALM inherit users' information and authorization profiles from an external repository, such as LDAP?

Answer

The information required for proper authentication is imported from LDAP.

Question

Is Role Management (access to different views and access and edit permission to separate parts) supported?

Answer

Yes, in ALM a permission module group represents the user role in the project. For details see the *About Managing User Groups and Permissions* section of the *ALM Administrator Guide*.

Question

Does ALM support limitations associated with user profiles and roles (for example, maximum number of group profiles, predefined profiles, and so on)?

Answer

ALM supports predefined user groups. For details see the *About Managing User Groups and Permissions* section of the *ALM Administrator Guide*.

Question

Is Access Control supported at Field Level?

Answer

Yes, you can define access control at the field level when defining group permissions. Also, workflow customization and data hiding further customize the access control at field level. For details, see the *ALM Administrator Guide*.

8 Data Integrity

Data integrity is a critical security requirement. The data backup procedure is an integral part of this requirement.

ALM does not provide backup capabilities. Following are some important considerations:

- Backup is especially important before critical actions such as project upgrade. See the *Back Up Projects in Existing ALM Installation* section of the *ALM Installation and Upgrade Guide* for details.
- Backup files should be stored properly according to the industry best practices to avoid unauthorized access.
- Since data backup consumes lots of resources, it is strongly recommended to avoid running backups during peak demand times.

Note: When backing up the database, ensure that the file repository is backed up at the same time to reflect the same system state.

9 Encryption Model

Transparent Data Encryption (TDE)

ALM and Performance Center are certified to work with Transparent Data Encryption (TDE) for Microsoft and Oracle databases. Implementation of TDE can have an impact on system performance. For details, contact the vendor providing encryption.

Full Disk Encryption (FDE)

Full disk encryption (FDE) is supported for all system components, including database, server, repository server, and client machines. Implementation of FDE can have an impact on system performance. For details, contact the vendor providing encryption.

ALM Encryption

ALM crypto capability is used to encrypt sensitive credentials and store them encrypted in the database. Examples of sensitive data include credentials to the database server ALM uses, credentials to the LDAP and SMTP servers with which ALM integrates, and credentials for machines that contain user data.

ALM crypto implementation uses the following security configuration:

JCE crypto source, Symmetric block cipher, 3DES engine, 192 key size

LW crypto source, Symmetric block cipher, AES engine, 256 key size

Password Encryption

User passwords are never stored, only the hash versions are stored.

FAQ

Question

Does ALM transmit account passwords in an approved encrypted format?

Answer

It is strongly recommended to enable SSL on the ALM and LDAP servers to ensure secured account password transmission.

Question

Does ALM store account passwords in approved encrypted format?

Answer

User passwords are not stored at all, only the hash; but internal system passwords are stored in AES 256.

Question

Does ALM use the Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules and random number generator to implement encryption, key exchange, digital signature, and hash functionality?

Answer

The cryptography provider used by ALM is not FIPS validated.

Question

What base product and service authentication methods are provided?

Answer

ALM can be configured to support one of the following authentication methods: user name and password, LDAP authentication, smartcard, and external authentication. For details, see the *ALM External Authentication Configuration Guide*.

Question

Is SSO (Single Sign On) supported?

Answer

Yes, based on the third-party SSO provider, such as Siteminder. For details, see the *ALM External Authentication Configuration Guide*.

Question

Does ALM integrate with Identity Management (via API or AD) for system and product users?

Answer

ALM integrates with IDM-SSO providers, such as Siteminder, where a remotely authenticated user name is passed in the header. This requires a separate configuration. For details, see the *ALM External Authentication Configuration Guide*.

Question

Are there any default vendor-supplied passwords or other security parameters embedded in ALM?

Answer

Yes, but the defaults can be replaced by configuration.

10 Logs

This chapter provides information related to logs.

Log and Trace Model

There are several types of logs provided on the ALM server:

- Client logs
- Site administration logs
- PPT project planning and tracking) logs

In addition, the history of changes to existing objects (defects, test cases, requirements, and so on) are stored in the database as history. This information remains as long as the object itself is not deleted. For this reason, we recommend using a dedicated folder as an alternative to permanent deletion.

Recommendations:

- Pay attention to the log level and do not leave the level at Debug.
- Pay attention to log rotation.
- Restrict access to the log directory.
- If logs archiving is needed, create your own archiving policy.

Log and Trace Security Administration and Features

Sensitive data is kept on log files. ALM provides applicative logs that can report all system events according to log level. It is the user's responsibility not to insert unprotected sensitive data to regular ALM entity fields.

The data provided in log files depends on the log level. For details, see the *Configuring Servers and Parameters* chapter of the *ALM Administration Guide*.

The period of time that log data is kept is configurable. The default is unlimited. The wrapper.log is configurable in the wrapper.conf file.

FAQ

Question

Does ALM audit access to need-to-know information and key application events?

Answer

The information can be obtained from the application log files or ALM entity history.

Question

Does ALM display the user's time and date of the last change in data content?

Answer

This information is available in ALM entity history for fields marked as History Enabled in project customization. For details, see the *Customizing Project Entities* section of the *ALM Administrator Guide*.

Question

Does ALM support the creation of transaction logs for access and changes to the data?

Answer

The information can be found in the application logs based on the log level. For details, see the *Configuring Servers and Parameters* chapter of the *ALM Administration Guide*.

11 General Questions

Question

How can I report security issues?

Answer

Via the following link:
https://h41268.www4.hp.com/live/index.aspx?qid=11503

Question

Where can customers obtain the latest information regarding security vulnerabilities in ALM?

Answer

You can obtain the latest information regarding security vulnerabilities and also register for alerts via this webpage:
https://h20566.www2.hp.com/portal/site/hpsc/public/kb/secBullArchive?ac.admitted=1389784040189.876444892.199480143

We appreciate your feedback

If you have comments about this document, you can *contact the documentation team* by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Secured Deployment and Configuration Guide (ALM 12.00)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to SW-Doc@hp.com.