JD Edwards EnterpriseOne Tools

Security Administration Guide

9.2

JD Edwards EnterpriseOne Tools
Security Administration Guide

9.2

Part Number: E53542-47

Contents

Preface

Welcome to the JD Edwards EnterpriseOne documentation.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc* .

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info* or visit *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs* if you are hearing impaired.

Related Information

For additional information about JD Edwards EnterpriseOne applications, features, content, and training, visit the JD Edwards EnterpriseOne pages on the JD Edwards Resource Library located at:

http://learnjde.com

Conventions

The following text conventions are used in this document:

Convention	Meaning
Bold	Boldface type indicates graphical user interface elements associated with an action or terms defined in text or the glossary.
Italics	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`Monospace`	Monospace type indicates commands within a paragraph, URLs, code examples, text that appears on a screen, or text that you enter.
> Oracle by Example	Indicates a link to an Oracle by Example (OBE). OBEs provide hands-on, step- by-step instructions, including screen captures that guide you through a process using your own environment. Access to OBEs requires a valid Oracle account.

1 Introduction to EnterpriseOne Security

Understanding this Guide

This guide contains comprehensive instructions and recommendations for setting up a secure EnterpriseOne environment. It contains pre- and post installation security considerations, as well as instructions on how to use EnterpriseOne security applications to ensure only authorized individuals have access to EnterpriseOne applications, features, and data.

This guide is organized into the following parts:

- **Part I, Security Overview Chapters** provide an overview of EnterpriseOne security, from secure architecture for an EnterpriseOne environment to application security.

  This part contains the following chapters:

  Chapter 1 - Introduction to EnterpriseOne Security

  Chapter 2 - General Principles of Security

- **Part II, Secure Installation and Configuration Chapters** provide guidelines for implementing a secure EnterpriseOne system architecture. This part contains pre-installation, installation, and post-installation tasks and recommendations related to security.

  Part II provides guidelines and recommendations for configuring and deploying JD Edwards EnterpriseOne to make it more secure in real-world, customer environments. It provides information about securing the overall infrastructure of a deployed EnterpriseOne system. It contains practical instruction for technical users, installers, and system administrators who implement and maintain the EnterpriseOne system. Part II also contains system hardening configuration recommendations, including hardening of the EnterpriseOne database and hardening of EnterpriseOne tools and administration applications.

  It is not possible to address every security scenario that might be applicable to a particular implementation and environment. Therefore, the items discussed in this part are intended to give a broad, best practices baseline for securing EnterpriseOne.

  This part contains the following chapters:

  Chapter 3 - Pre-Installation Security Considerations

  Chapter 4 - Securing EnterpriseOne System Components

  Chapter 5 - Post-Installation Security Configurations

  Chapter 6 - Security for Custom Map Viewers

  Chapter 7 - Managing Data Source Security

  Chapter 8 - Encrypting Sensitive Data in EnterpriseOne

- **Part III, EnterpriseOne Access Provisioning Chapters** describes how to set up user and role profiles in EnterpriseOne so that you can configure sign-in security and object-level security for EnterpriseOne users.

  Access provisioning is the process of setting up user and role profiles in EnterpriseOne in order for users to gain access to EnterpriseOne and the particular applications and features they are authorized to use. After you set up user and role profiles, you can create sign-in security records for each user. You also have the option to set up a single sign-on configuration or configuring EnterpriseOne to manage users through third-party, LDAP-enabled systems. See Part IV, "EnterpriseOne Authentication Security" for more information.

  In addition, you use user and role profiles to create security records for authorizing access to particular EnterpriseOne applications, features, and data. See Part V, "EnterpriseOne Authorization Security" for more information.

  This part contains the following chapters:

  Chapter 9 - Provisioning User and Role Profiles

  Chapter 10 - Setting Up Long User IDs in EnterpriseOne

- **Part IV, EnterpriseOne Authentication Security** describes how to implement sign-in security so that only authenticated users have access to JD Edwards EnterpriseOne. It also provides instructions for setting up single sign-on and managing users through a third-party LDAP directory.

  EnterpriseOne authentication security ensures that anyone who attempts to sign in to EnterpriseOne is a valid, authenticated EnterpriseOne user.

  In addition to setting up sign-in security, authentication security encompasses configurations for single sign-on, managing users and passwords in an LDAP-compliant directory service, and unified logon (prior to release

9.2.2 only). It is important that you carefully follow the instructions as you implement any of the configurations discussed in this part.

This part contains the following chapters:

Chapter 11 - Understanding Sign-in Security

Chapter 12 - Setting Up User Sign-in Security

Chapter 13 - Enabling Long Passwords in EnterpriseOne

Chapter 14 - Enabling LDAP Support in JD Endwards EnterpriseOne

Chapter 15 - Setting Up JD Edwards EnterpriseOne Single Sign-On

Chapter 16 - Setting Up JD Edwards EnterpriseOne Single Sign-On Through Oracle Access Management 11g Release 2

Chapter 17 - Setting Up JD Edwards EnterpriseOne Single Sign-On Through Oracle Access Management 12c

Chapter 18 - Using Oracle Access Manager to Enable Support for Windows Native Authentication with EnterpriseOne

Chapter 19 - Configuring Long User ID and Password Support in a Single Sign-On Configuration with Oracle Access Manager

Chapter 20 - Configuring SSL/TLS for JDENET

Chapter 21 - Configuring SSL for EnterpriseOne Servers

- **Part V, EnterpriseOne Authorization Security** describes how to set up authorization security, which includes setting up EnterpriseOne object-level security using the Security Workbench. It also describes other EnterpriseOne security features such as Address Book Data security and user defined objects security.

  This part contains the following chapters:

  Chapter 22 - Understanding Authorization Security

  Chapter 23 - Setting Up Authorization Security with Security Workbench

  Chapter 24 - Managing Security for User Defined Objects

  Chapter 25 - Setting Up JD Edwards Solution Explorer Security

  Chapter 26 - Setting Up Address Book Data Security

  Chapter 27 - Setting Up Business Unit Security

  Chapter 28 - Upload and Download Security

- **Part VI, EnterpriseOne Developer Security** describes how to set up security for developers which includes defining the actions that developers can perform in the Object Management Workbench.

  The Object Management Workbench (OMW) in EnterpriseOne is the primary component of the change management system for EnterpriseOne development. A change management system is vital to a productive development environment because it helps organize a myriad of development activities and helps prevent

problems, such as when a developer intermixes components from different releases or when multiple developers simultaneously change an object. OMW automates many of these change management activities.

As part of the OMW implementation, it is critical that you set up permissions to determine who can access OMW, as well as set up and assign OMW users to roles that control the actions that they can perform.

This part contains the following chapter:

Chapter 29 - Configuring OMW User Roles and Allowed Actions

- **Part VII, EnterpriseOne Security Auditing** describes how to run reports that are used for security auditing purposes. It also provides an overview of the EnterpriseOne auditing features for supporting the 21 CFR Part 11 auditing regulations.

  This part contains the following chapters:

  Chapter 30 - Configuring EnterpriseOne Security Auditing

  Appendix A - DB Password Encryption

  Appendix B - Creating a JD Edwards EnterpriseOne LDAP Configuration for OID

  Appendix C - JD Edwards EnterpriseOne Cookies

  Appendix D - Default Database User Accounts

Introduction to EnterpriseOne Security

Oracle's JD Edwards EnterpriseOne Tools provides security applications, reports, and features to help you protect your company's sensitive application data. EnterpriseOne authentication security ensures that only authenticated users can sign in to EnterpriseOne. Authorization security ensures that EnterpriseOne users have access to only the applications and features that they are authorized to use.

In addition, EnterpriseOne enables you to set up security for developers who use Object Management Workbench (OMW) to add and modify objects for custom applications. Setting up developer security ensures that developers can only perform certain actions in OMW based on pre-defined responsibilities.

EnterpriseOne also includes reports that you can use for security auditing purposes, as well as auditing features for supporting the 21 CFR Part 11 auditing regulations.

Before you use the EnterpriseOne administration applications to properly set up authentication security, authorization security, developer security, and security auditing, it is important that the overall infrastructure of a deployed JD Edwards EnterpriseOne system is properly secured. See *Secure Installation and Configuration*in this guide for more information.

Concepts and Terminology

You should familiarize yourself with the following terms and concepts before reading the contents of this guide:

Access provisioning

The process of setting up user and role profiles in EnterpriseOne for sign-in security (authentication) and authorization security.

Authentication

The process of verifying that users signing into EnterpriseOne are valid EnterpriseOne users.

Authorization

The process of granting or denying users access to EnterpriseOne applications, features, data, and data sources. In EnterpriseOne, most authorization security is applied at the object level through Security Workbench.

Object-level security

A type of authorization security that enables you to secure specific EnterpriseOne objects such as applications, forms, and various other EnterpriseOne features. Object-level security provides flexibility and a higher level of security integrity.

Developer security

Security that determines the actions developers can perform when customizing or developing EnterpriseOne applications in Object Management Workbench (OMW). Actions can include checking out and checking in objects, promoting objects, transferring objects, removing objects, and so forth. OMW's automation relies on an administrator who carefully configures these actions.

Security auditing

EnterpriseOne contains a set of reports and tools than enable you to audit sign-in security records (for authentication) and object security records (for authorization), as well other security-related information. In addition, EnterpriseOne contains electronic signature and auditing tools that enable your organization to comply with the FDA 21 CFR Part 11 regulation for submitting electronic records.

Data encryption

The process of transforming information into code so that it cannot be read by a third-party system. EnterpriseOne encrypts user passwords stored in the database.

Data privacy

In EnterpriseOne, Address Book data security enables you to restrict users from viewing Address Book information that is determined as private, personal data. An administrator can use the Address Book Data Permissions application (P01138) to set up Address Book data security.

Data masking

Customizing a field so that specified characters are embedded in place of sensitive data that appears in applications. This prevents sensitive data from being displayed to unauthorized users. A developer enables data masking through the Data Dictionary application (P92001), which is part of the EnterpriseOne suite of development tools used to customize or create customized applications. For more information about data masking, see *"Display Rule" in the JD Edwards EnterpriseOne Tools Data Dictionary Guide*.

Secure Socket Layer (SSL)

A security protocol that you can apply to various EnterpriseOne servers that provides communication privacy. SSL enables client and server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

***PUBLIC**

A special ID within EnterpriseOne that automatically includes all users within it. This option controls security for all users who are designated by ID type ***PUBLIC** in the User or Role field. You can use this ID to apply security even if you do not have a specific record set up for it in user profiles.

Security overrides

Security records that operate as exceptions to existing security records. Security overrides specify that users are *unsecured* from an EnterpriseOne object. In other words, security overrides allow users access to a particular object, even if another security record in the system specifies that access is not allowed.

2 General Principles of Security

General Principles of Security

Follow these general principles of security when configuring and maintaining the EnterpriseOne system.

Apply Latest Patch

One of the principles of good security practices is to keep all software versions and patches up-to-date. Establish a policy to keep track of all the vendors-including Oracle-that have supplied software for the production environment. Also, identify the latest software patches and apply them regularly. Refer to the minimum technical requirements (MTR) and any restrictions for the software you are using when applying patches. For JD Edwards EnterpriseOne minimum technical requirements information, see document 745831.1 (JD Edwards EnterpriseOne Minimum Technical Requirements Reference) on My Oracle Support:

https://support.oracle.com/rs?type=doc&id=745831.1

Apply Oracle Critical Patch Update

Oracle releases information (and patches) for security issues for most products through quarterly, bundled, integrated Critical Patch Updates (CPU). JD Edwards EnterpriseOne Tools security patches are also released with the quarterly Oracle CPU; these patches are normal tools one-off service packs.

Patches can include fixes for the operating system, database, web application server, as well as any EnterpriseOne server. Refer to the Certifications tab on My Oracle Support and search for the EnterpriseOne components:

https://support.oracle.com/epmos/faces/CertifyHome?_adf.ctrl-state=eyjh3ekv3_9&_afrLoop=303034385433646

CPUs include fixes for the most critical security issues, fixes to avoid patch conflict, or prerequisites for security fixes. The release dates for CPUs are announced a year in advance and are selected based on most customers' financial calendars. Oracle tries to avoid the blackout dates during which customers generally do not touch their financial systems.

Refer to the Oracle Critical Patch Updates and Security Alert website for more information:

http://www.oracle.com/technology/deploy/security/alerts.htm

Monitor System Activity

One of the main requirements of system security is monitoring. Auditing and reviewing audit records address this requirement. Each component within a system has some degree of monitoring capability. Establish a policy to check

and monitor activities in your system regularly. Refer to the database and operating system documentation for audit functionality. For JD Edwards EnterpriseOne, follow the advice in this document and regularly monitor audit records.

Configure Accounts Securely

Good security requires secure accounts. Establish a policy to set up strict password controls for all accounts including the database, operating system, and JD Edwards EnterpriseOne so that passwords are not compromised. Often, people use passwords associated with them, such as license plate numbers, children's names or a hobby. In addition, establish a policy to periodically change passwords.

Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Over ambitious granting of responsibilities, roles, and permissions, especially when people are few and work needs to be done quickly, often leaves a system wide open for abuse. You should initially establish a policy to determine and assign least privileges to users. Periodically review user privileges to determine relevance to current job responsibilities.

Enable Minimum Level of Logging

Always run the JD Edwards EnterpriseOne and other systems with a minimum level of logging in the production environment. Running JD Edwards EnterpriseOne with a debug level of logging in the production environment adversely impacts system performance as well as it logs unnecessary sensitive information about the environment. Furthermore, the logs can be used to exploit the system if a malicious user obtains access to the log files.

Set Up Change Management Process

Establish a policy to set up a change management process to keep track of all the changes in your software systems. All changes should be approved and audited.

3 Pre-Installation Security Considerations

Recommendations for Deploying and Configuring JD Edwards EnterpriseOne in a Secure Environment

In today's environment, a properly secured computing infrastructure is critical. As companies expand, so does the complexity of their business processes. In an internet environment, the risks to valuable and sensitive data are greater than ever before. In addition, a company's computing infrastructure grows as more third-party products are integrated with its enterprise software. As a result, this type of environment can create potential security gaps.

It is critical that you secure a JD Edwards EnterpriseOne environment in alignment with your company's enterprise security policies. Those policies should be created based upon your established security model. When securing an EnterpriseOne environment, you should take a comprehensive approach that is in concert with the overall corporate security policies, guidelines, and business requirements.

It is important that EnterpriseOne and the various components involved in an EnterpriseOne setup are properly secured. This ensures that EnterpriseOne applications deliver data in a secure and reliable fashion so that data integrity, confidentiality, and availability are maintained. JD Edwards EnterpriseOne Tools must be installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

EnterpriseOne Upgrade Security Considerations

The JD Edwards EnterpriseOne Upgrade guides contain security-related tasks that you must perform when upgrading the production environment in EnterpriseOne. See the following sections in the Upgrade guides in the JD Edwards EnterpriseOne Installation and Upgrade Documentation Library:

- "General Checklist and Considerations"
- "Adding Security Overrides"

Use the following link to access the JD Edwards EnterpriseOne Upgrade guides:

http://docs.oracle.com/cd/E61420_01/index.htm

Lock Database User Accounts for Previous Releases

If you are upgrading a JD Edwards EnterpriseOne Applications release, delete or lock all the database accounts used by previous EnterpriseOne releases.

Network Infrastructure Security

In an internet environment, securing the network infrastructure is the foremost priority for an organization because the risks to valuable and sensitive data are greater than in a WAN environment. To eliminate potential weak points in the

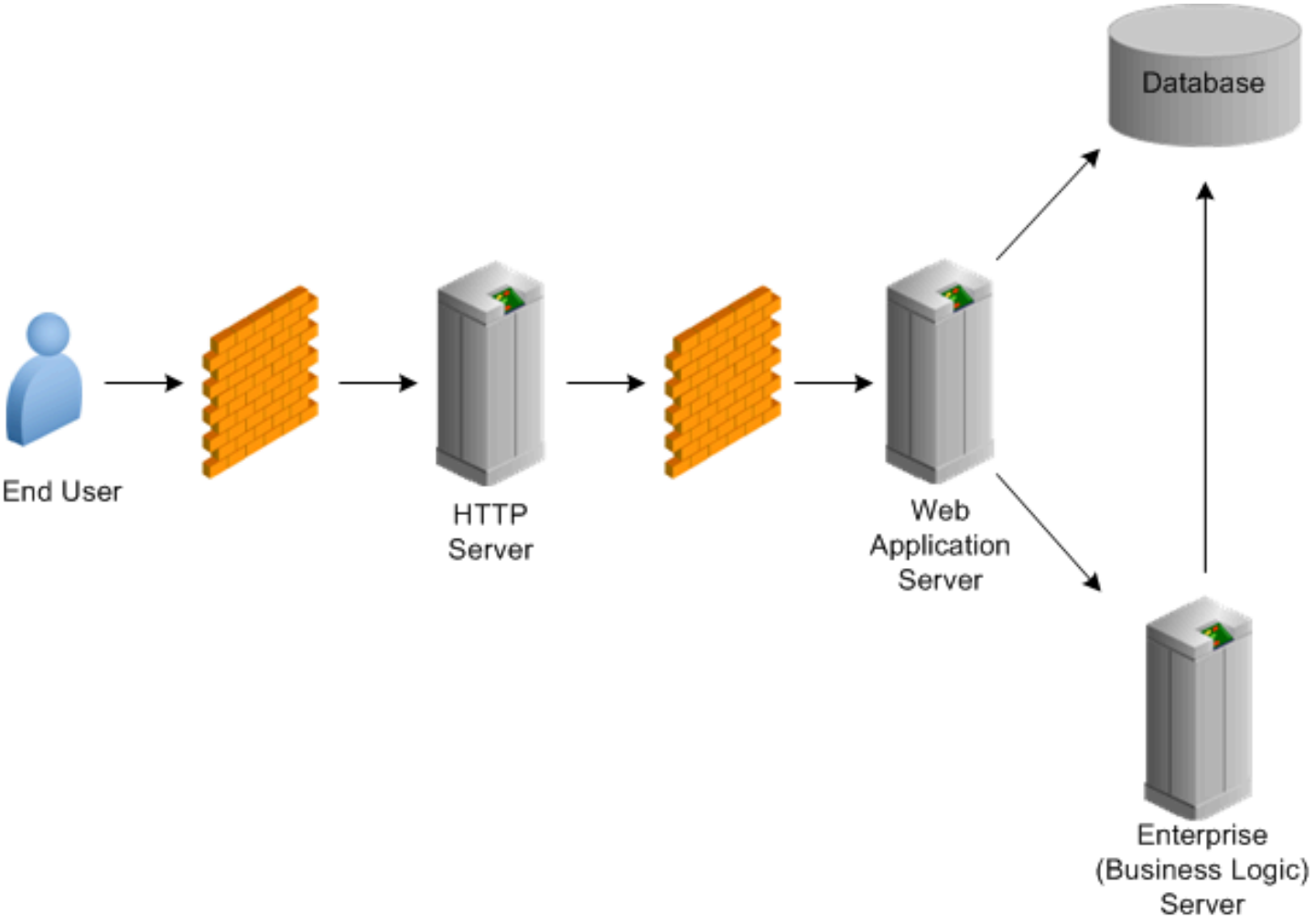
network infrastructure, you may opt to pass data from protocol to protocol without the complexity of decryption and encryption. To do so securely, you must have some way to securely transfer data across network protocol boundaries. The internet enables you to connect your corporate intranet to a broad public network. Although this capability provides enormous business advantages, it also poses a risk to your data and your computer system. One way of protecting the privacy and integrity of your system is to place a firewall between the public network and your intranet.

Set Up Firewall and DMZ

A firewall is one of the most common network devices used to secure a network environment. Set up a firewall and demilitarized zone (DMZ) to block unauthorized traffic. You should place the EnterpriseOne HTTP server in a DMZ configuration for internet facing systems. Keep the web application server, database, and Enterprise Server (otherwise known as the business logic or security server) behind a firewall. Firewalls provide assurance that access to these systems is restricted to a known network route that can be monitored.

In addition, you can also place a firewall between the Web Application Server and the database or Enterprise Server to add an additional layer of protection. See *Additional Network Infrastructure Security* for more information.

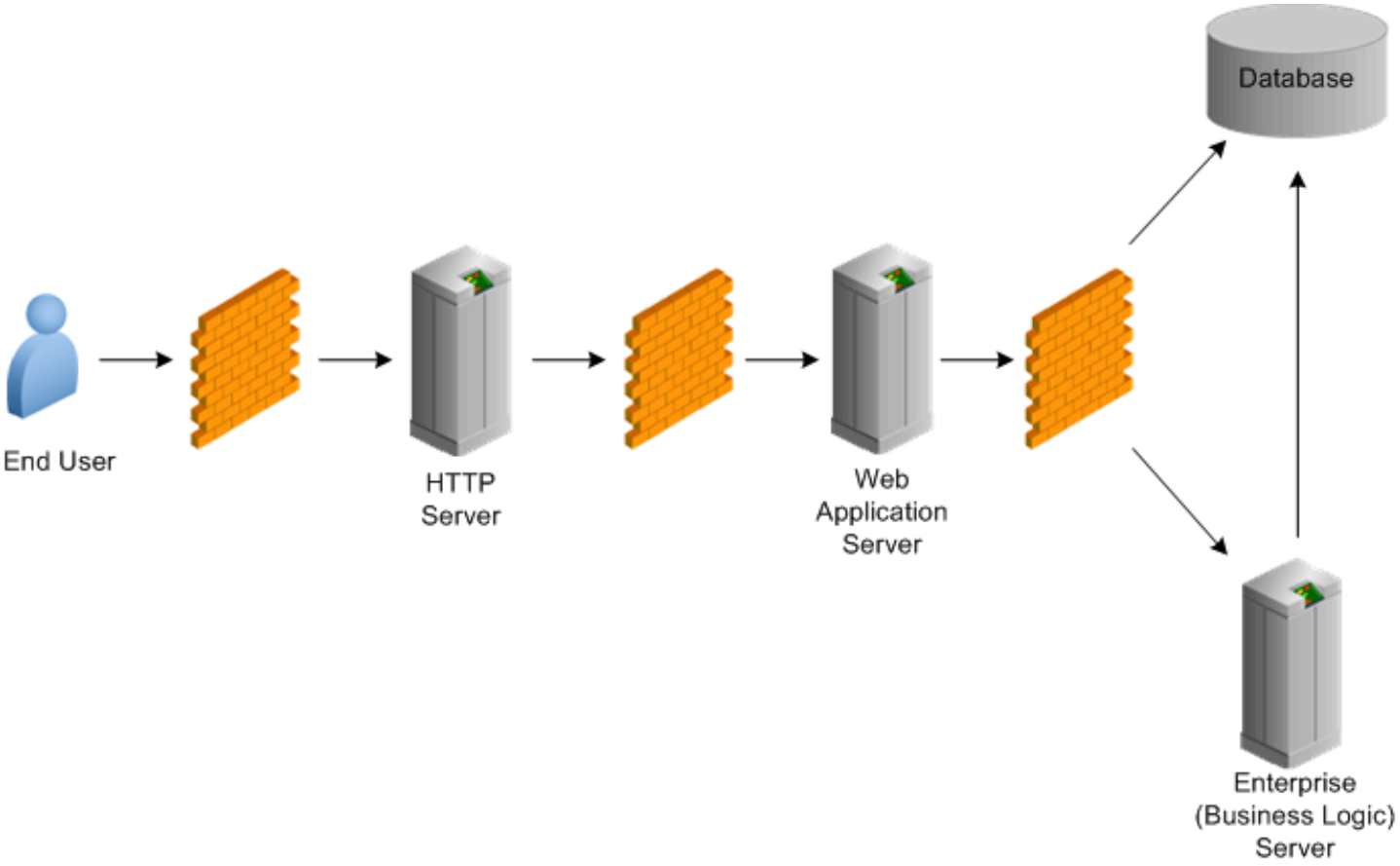
This illustration shows the recommended firewall setup for JD Edwards EnterpriseOne:



You should also install an Intrusion Detection System (IDS) and establish a policy to regularly monitor unauthorized traffic.

Additional Network Infrastructure Security

For an internet facing system, it is recommended that you place the HTTP server in a DMZ zone and keep the EnterpriseOne HTML Server (Web Application Server), database, and Enterprise Server behind a firewall. In addition, you can add an additional layer of protection by placing a firewall between the Web Application Server and the database or Enterprise Server.



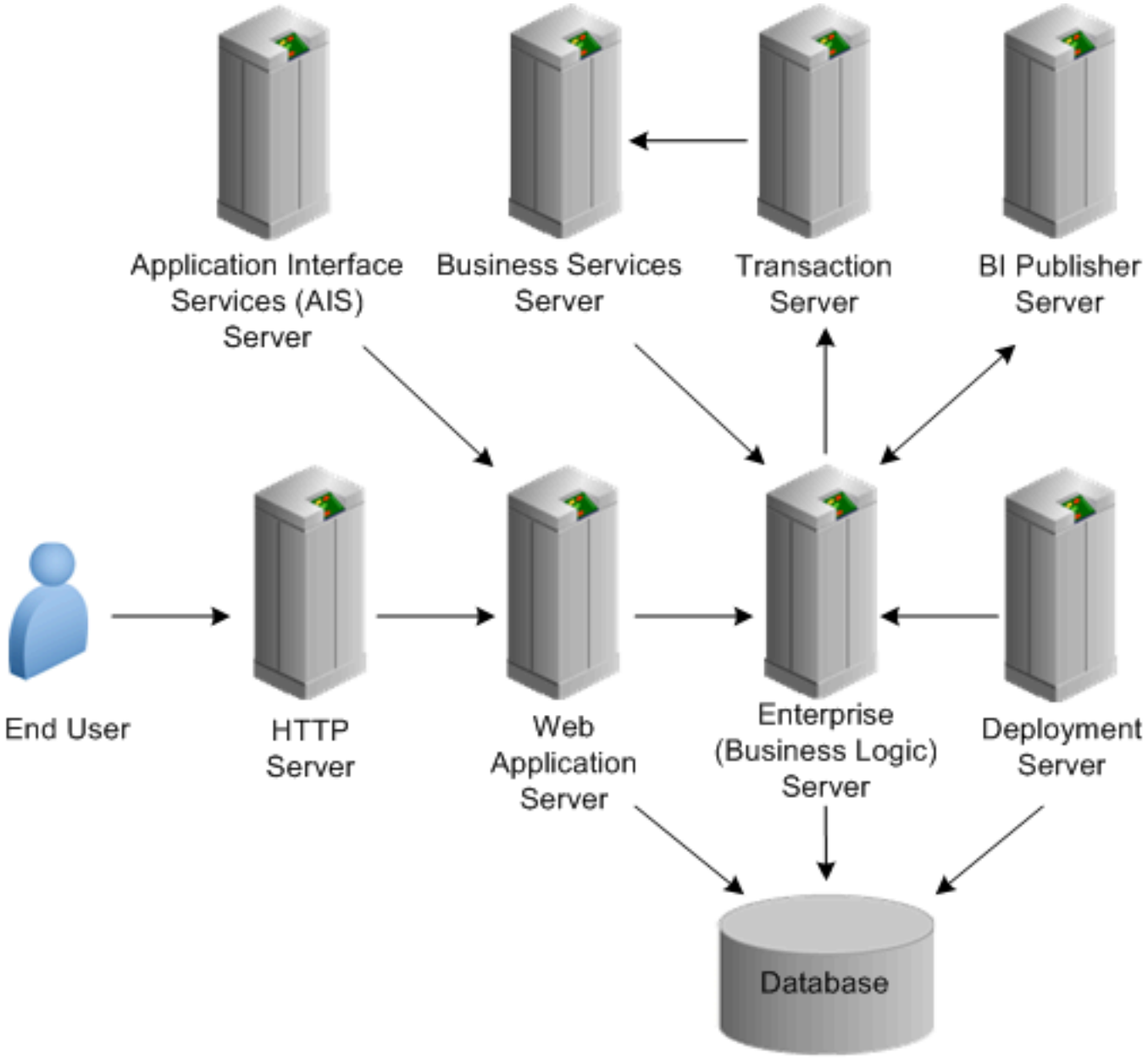
Enable Predefined JDENET Ports in JDE.INI

When there is a firewall between the EnterpriseOne HTML Server and the Enterprise Server, set the PredfinedJDENETPorts setting to 1 in the JDE.INI file of the Enterprise Server. This setting enables JDENET network process to use a predefined range of TCP/IP ports. This port range starts at the port number that is specified by serviceNameListen and ends at the port that is calculated by the equation serviceNameListen = maxNetProcesses - 1. You must open these ports in a firewall setup to successfully connect the EnterpriseOne HTML Server to the Enterprise Server.

4 Securing EnterpriseOne System Components

Overview of JD Edwards EnterpriseOne System Components

This illustration shows the various components of a JD Edwards EnterpriseOne configuration:



Database Security

EnterpriseOne stores all system and business data in a supported relational database.

During a Platform Pack installation, the installer creates two initial roles (referred to as group profiles on iBMi and groups on UDB) that define access to data source tables. You must make sure that these roles are set up in EnterpriseOne before completing the installation. If the database administrator defines additional roles for securing access to tables in the data source, you need to make sure that these roles are defined in the EnterpriseOne Data Source application as well. See *Managing Data Source Security* in this guide for details.

For a **new** EnterpriseOne installation, the Platform Pack Installer uses these roles for all tables, including system and business data in the database.

For an **upgrade**, the Platform Pack Installer applies the roles to secure access to system tables only. It does not apply the roles to the business data or control tables. For these tables, you can use one of the following methods to apply the security:

- In the business data and control tables data source, set up roles for a database administrator and database user. Add these same roles to the Grant Data Source Privileges (P986117) application in EnterpriseOne. See *Managing Data Source Security* in this guide for details. (Recommended)

  OR

- Modify the scripts the Platform Pack Installer uses to apply data source security to system tables and then run these scripts over the business data and control tables data source. Make sure the roles used in the script for the data source security are added to Grant Data Source Privileges (P986117) application in EnterpriseOne.

  OR

- Run the script for your platform as described in *Revoke PUBLIC Access to Installed EnterpriseOne Database Tables*.

  This last option is not recommended because if an OMW user updates a table, the security is lost and will have to be reapplied by running the script again. Only the first two options ensure that the security persists in the data source for any table modifications.

Revoke PUBLIC Access to Installed EnterpriseOne Database Tables

JD Edwards EnterpriseOne Applications release 9.1 and prior include database Platform Packs that install EnterpriseOne tables with PUBLIC level access. PUBLIC acts as a default role granted to every database user. Oracle provides platform specific tools to revoke PUBLIC access from EnterpriseOne database tables. Implementing the platform specific tools enables you to ultimately grant access for each database table to one or more database roles while revoking access to PUBLIC. The database roles will be associated to each EnterpriseOne system (proxy) user as deemed appropriate. This ensures that the database tables are accessible by only database users associated to a particular database role.

The following sections provide links for the platform-specific tools that you can use to revoke PUBLIC access from EnterpriseOne tables for the supported databases: Oracle, Microsoft SQL Server, and IBM databases.

EnterpriseOne PUBLIC Shutdown Scripts for Oracle Database

Oracle provides a set of scripts in SAR 8289283 that you can run to revoke PUBLIC access in EnterpriseOne tables installed in an Oracle Database. See Doc ID 748163.1 in My Oracle Support for instructions on how to download SAR 8289283 and run the scripts. Use the following URL to access and sign in to My Oracle Support:

https://support.oracle.com

EnterpriseOne PUBLIC Shutdown Scripts for Microsoft SQL Server

Oracle provides a set of scripts in SAR 8090565 that you can run to revoke PUBLIC access in EnterpriseOne tables installed in a Microsoft SQL Server Database. See Doc ID 748159.1 in My Oracle Support for instructions on how to download SAR 8090565 and run the scripts. Use the following URL to access and sign in to My Oracle Support:

https://support.oracle.com

DB2 for i PUBLIC Shutdown Using SETOWAUT

Oracle provides a SETOWAUT toolkit for the IBM i platform that enables you to restrict access to database tables to only EnterpriseOne authorized users. The SETOWAUT toolkit is the equivalent PUBLIC shutdown methodology for the IBM i platform. Furthermore, the EnterpriseOne middleware and command set used to control the EnterpriseOne solution is also restricted permitting only authorized users to control and use this comprehensive program set. For instructions on how to the use of the SETOWAUT toolkit, see *"Administering JD Edwards EnterpriseOne Database Security for IBM i" in the JD Edwards EnterpriseOne Administration Guide* .

Limit Access to Query Tools

Database user passwords should be strong and end users should have limited access to Query Tools.

File System Security

The *JD Edwards EnterpriseOne Administration Guide* contains security instructions for UNIX and Microsoft Windows servers that you must follow to ensure that only certain EnterpriseOne files can be accessed by the operating system. See the following sections for more information:

- *"Maintaining File Security for UNIX and Linux"*
- *"Maintaining File Security for Windows"*

Encryption of Sensitive Information in Configuration Files

Sensitive information such as passwords can be encrypted in EnterpriseOne configuration (ini) files. See *Encrypting Sensitive Data in EnterpriseOne* in this guide for more information.

Deployment Server Security

The Deployment Server typically contains EnterpriseOne source code, package build areas, install packages, and licensing information.

You can configure the deployment server with the Secure Sockets Layer (SSL) protocol so that all communication is over HTTPS. Starting with EnterpriseOne Tools 9.2.5.1, the SSL setting for the deployment server in server manager is enabled for SSL by default. Therefore, you need to ensure that the deployment server is configured for SSL. This configuration requires a certificate signed by a certificate authority to establish secure communication between servers. See *Chapter 21, Configuring SSL for EnterpriseOne Servers*.

Limit Access to System

Use these guidelines when setting up security for the Deployment Server:

- Only allow system administrators to log on to the Deployment Server.
- Do not place shared services such as printing or DNS services on this host.
- Run only EnterpriseOne on this machine for software installs and upgrades.
- Do not create user accounts on this machine.
- Give full access to the media object queue directory for only one user account that is accessing this directory from the EnterpriseOne HTML Server when you are not accessing media objects from a Microsoft Windows client.
- Limit access to PrintQueue directory.

Secure Configuration File

The Deployment Server configuration file (JDE.INI) might contain the override password for the default database user to connect to EnterpriseOne data sources when doing an installation, upgrade, or applying a software update. Therefore, you need to secure this file using operating system security such as Microsoft Windows security, UNIX object security, or IBM i object security. After a successful install, upgrade, or software update, remove the [DSPWD] section from JDE.INI.

Secure Log Files

You should give only certain users access to view Deployment Server log files (error and debug), as these files might contain sensitive information about the user and location of the database.

JD Edwards EnterpriseOne Enterprise Server Security

The Enterprise Server (otherwise known as the business logic server) is used as middleware to run various functions such as business functions and reports. In addition, it functions as the security server. You must secure this server so that only configurable network computing (CNC) administrators have access to it.

You can configure the Enterprise Server with the Secure Sockets Layer (SSL) protocol so that all communication is over HTTPS. Starting with EnterpriseOne Tools 9.2.3, the SSL setting for the Enterprise Server in Server Manager is enabled for SSL by default. Therefore, you need to make sure the Enterprise Server is configured for SSL, which requires a certificate signed by a certificate authority to establish secure communication between servers. See *Chapter 21, Configuring SSL for EnterpriseOne Servers*.

Limit Remote Access

You should prohibit or severely limit remote session access and remote session control for the Enterprise Server.

Secure Configuration File

The Enterprise Server configuration file (JDE.INI) contains the user ID and password. Therefore, you should secure this file using operating system security such as Microsoft Windows security, UNIX object security, or IBM i object security.

> **CAUTION:** Implementing security on these files will prevent Server Manager from modifying configuration settings within these files.

Limit Access to Administer EnterpriseOne Services

You should give only certain users authority to start and stop EnterpriseOne processes and to run scripts because this authority also requires access to the JDE.INI file, which contains the database password. Do not give users access to update EnterpriseOne script files for starting and stopping services.

Secure Log Files

You should give only certain users access to log files (error and debug) on the Enterprise Server. These files might contain sensitive information about the user and the location of the database.

> **CAUTION:** Implementing security on these files will prevent Server Manager from being able to display the logs.

Limit Access to BSFN Trace Logs

Change the ClientLog setting to 0 in the [DEBUG] section of the JDE.INI so that Call Object kernel does not send the business function (BSFN) server logs back to the workstation after executing the BSFN calls. For more information about this setting, refer to the JD Edwards EnterpriseOne Upgrade Guide for your platform located at:

http://docs.oracle.com/cd/E61420_01/index.htm

Limit Access to PrintQueue Directory

The Enterprise Server stores all the report output in the PrintQueue directory. You should give only certain users access to the PrintQueue directory.

Use Security Server

In a production environment, always use the security server. You can run business logic on the Enterprise Server without using a security server when logged in with a user ID that is also a database user.

JD Edwards EnterpriseOne HTML Server Security

The JD Edwards EnterpriseOne HTML Server is a critical component of the EnterpriseOne system. It is used as a gateway by all web users to access EnterpriseOne. EnterpriseOne supports Oracle WebLogic Server and IBM WebSphere Application Server for a web solution.

Oracle WebLogic Server

If you have deployed an Oracle WebLogic Server, take the appropriate steps to make the installation more secure. See *"Security" in the Oracle Fusion Middleware Information Roadmap for Oracle WebLogic Server* document.

IBM WebSphere

If you have deployed an IBM WebSphere Application Server, follow IBM's recommendations to make the installation more secure:

http://www.redbooks.ibm.com/abstracts/sg247660.html (WebSphere 7)

http://www.ibm.com/developerworks/websphere/zones/was/security/ (WebSphere 8.5)

Secure Configuration Files

The EnterpriseOne HTML Server uses these configuration files:

- JAS.INI
- JDBj.INI
- JDELOG.PROPERTIES

In addition, the web server can have a Tokengen.ini in a single sign-on environment. These files contain sensitive information that should not be available to all users, so you should use operating system security to secure the files.

> **CAUTION:** Implementing security on these files will prevent Server Manager from modifying configuration settings within these files.

Secure Log Files

You should give only certain users access to log files (error and debug) on the EnterpriseOne HTML Server. These files might contain sensitive information about the user and the location of the database.

> **CAUTION:** Implementing security on these files will prevent Server Manager from being able to display the logs.

J2EE Session Timeout Setting

After a user signs in, he or she can stay connected as long as the sign-in time allows and as long as the browser does not sit idle for longer than the timeout interval. A timeout interval specifies how long the user's machine can remain idle before the J2EE application server automatically disconnects the user from the application.

Set up a policy for inactive session timeout and set this value accordingly. For the web application server, this value is 30 minutes by default. For more information about setting the timeout values, refer to the *JD Edwards EnterpriseOne Tools HTML Server Reference Guide* for your platform located at:

http://docs.oracle.com/cd/E61420_01/index.htm

Limit Access to Media Object Queue Directory

The EnterpriseOne HTML Server caches the media object files under `/jde/moqueue/` directory of the installed web application. The operating system user for whom the web application server process is running must have full access to this directory. Secure access for all other users to this directory on the web server. You should use media object security in EnterpriseOne to secure access to media object attachments from EnterpriseOne applications. Refer to *Setting Up Authorization Security with Security Workbench* in this guide for more information on setting up media object security.

Set Up FTP User Access to Media Objects

You can configure the system to use Windows NT Share or FTP protocol to access media object files from media object queue directories. The FTP user ID and password should be provided in the JAS.INI file. You can enable FTP for media objects through the Media Object FTP Mode setting. This setting is part of the EnterpriseOne HTML Server settings that you can configure in Server Manager.

The FTP user or operating system user (in case of Windows NT Share) for whom the web server process is running should have full access to media object queue directories. You should limit the access to any other directories on the server where the media object queue directories are located for this FTP user or operating system user.

All other users should not have access to media object queue directories when users are not accessing media objects from the Windows client.

Set Up Secure FTP (SFTP) for Media Object Access

Oracle recommends using SSH file transfer protocol, otherwise referred to as Secure FTP (SFTP), for accessing media objects as a more secure alternative to FTP. When EnterpriseOne is configured to use SFTP for media objects, users can securely upload, download, and delete media objects.

When using SFTP, make sure that the SFTP user home folder is the same as the FTP user home folder for media object operations.

To enable SFTP, configure the following HTML Server settings located in the Web Runtime group settings in Server Manager:

- **Use Secure FTP for MediaObject Fetch**. Click this check box to use SFTP to access media objects.
- **Timeout for SFTP connection**. The amount of time, in milliseconds, the EnterpriseOne web client will wait to make a secure SFTP connection. If you receive a connection timeout error while connecting to SFTP, increase the timeout value.

> **Note:** If you are using Cygwin SFTP, make sure you add the following setting to the /etc/sshd_config file:
> `KexAlgorithms diffie-hellman-group1-sha1`

For details about the configuration settings mentioned in this section, refer to the Server Manager internal help for each setting. For information on how to access the configuration settings in Server Manager, see the *JD Edwards EnterpriseOne Tools Server Manager Guide* .

Use SSL (HTTPS) Between Browser and Web Server

Information sent over the network and across the internet in clear text can be intercepted. The Secure Socket Layer (SSL) protocol developed by Netscape Corporation is an industry-accepted standard for network transport layer security. SSL is supported by all currently available web servers and web browsers. You should configure SSL on the EnterpriseOne HTML Server, especially in an internet environment.

You can configure the EnterpriseOne HTML Server with the Secure Sockets Layer (SSL) protocol so that all communication is over HTTPS. See *Configuring SSL for EnterpriseOne Servers*.

Disable non-secure HTTP on the web application server after making sure that HTTPS is set up and working properly. Refer to the *Network Infrastructure Security* section in this guide for information about setting up network security in an internet environment.

HTTP Server Level

This section contains security considerations for the HTTP Server on the EnterpriseOne HTML Server.

Turn Off Directory Listing

Directory indexes display the contents of a directory if there is no index.html or similar file available. Disabling this entry prevents an intruder from viewing the files in a directory and potentially finding a file that could provide access to the system. Refer to the HTTP Server documentation to disable this feature in the web server configuration file.

Disable HTTP TRACE

The HTTP TRACE request method causes data to be returned to the client after it is retrieved by the server. The TRACE process can open up the system to malicious applications that can send the information to a third party site. Therefore, it is recommended that you disable HTTP TRACE. Refer to the security documentation for your application server for more information.

Deprecate Old Certificates

Certificates have a specified period of time in which they are valid. After the specified period of time has passed, a new certificate must be issued. Therefore, you should delete old certificates, as well as delete any certificates that have become compromised or corrupted.

Denial-of-Service Attacks

Denial-of-service (DOS) attacks can occur when a large number of poorly formed requests are sent to servlets. You can reduce the impact of DOS attacks, but it is impossible to prevent them. If an attacker throws enough data at a server to continuously use all the available network bandwidth, it will crowd out legitimate traffic, regardless of how the software is configured. Denial of service can only be handled at an application server level. To configure to reduce the impact of denial of service attacks, refer to the security documentation for your application server.

Portal Server Security

EnterpriseOne provides single sign-on support from the Collaborative Portal (IBM Portal) and Oracle WebCenter Spaces. Both portals use token-based authentication for achieving single sign-on with EnterpriseOne.

Refer to *Setting Up JD Edwards EnterpriseOne Single Sign-On* for more information.

Collaborative Portal

A single sign-on token is generated by Collaborative Portal. You should set up a new node to support single sign-on for the Collaborative Portal server. You can create a single sign-on node configuration using the EnterpriseOne SSO application.

Oracle recommends setting up an SSL configuration for the Collaborative Portal. For instructions, see "Configuring the WSRP Consumer portal for SSL" on the IBM WebSphere Portal website:

http://www-10.lotus.com/ldd/portalwiki.nsf/xpDocViewer.xsp?lookupName=IBM+WebSphere+Portal+7+Product+Documentation#action=openDocument&res_title=Securing_WSRP_by_SSL_for_a_Consumer_portal_wp7&content=pdcontent

Oracle WebCenter Spaces

With an EnterpriseOne single sign-on setup for Oracle WebCenter Spaces, a single sign-on token is generated by the EnterpriseOne provider server. The provider server can be an Oracle WebLogic Server or IBM WebSphere Application Server and can be used as a standalone HTML Server. You should set up a new node for supporting single sign-on from the provider server. You should create a single sign-on node configuration using the EnterpriseOne SSO application.

The TokenGen.ini file contains node name and node password in plain text. You need to secure this file using operating system security.

In addition to the above recommendations, follow the guidelines in the *JD Edwards EnterpriseOne HTML Server Security* section in this guide to secure your web environment.

Oracle recommends setting up an SSL configuration for Oracle WebCenter Spaces. For instructions, see "Securing the Spaces Connection to Portlet Producers with SSL" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*:

https://docs.oracle.com/cd/E28280_01/webcenter.1111/e12405/wcadm_security_ssl.htm#WCADM6449

Transaction Server Security

EnterpriseOne event functionality provides an infrastructure that can capture EnterpriseOne transactions in various ways and provides real-time notification to third-party software, end users, and other Oracle systems such as Customer Relationship Management (CRM).

You can configure the Transaction Server with the Secure Sockets Layer (SSL) protocol so that all communication is over HTTPS. See *Configuring SSL for EnterpriseOne Servers*.

Secure Configuration Files

The Transaction Server uses the bootstrap user and password from JDBj.INI in `install_directory/E1TranSrv/cfg` directory. Secure this file, as well as other configuration files (JAS.INI and JDELOG.PROPERTIES), using operating system security.

CAUTION: Implementing security on these files will prevent Server Manager from modifying configuration settings within these files.

Secure Log Files

You should give only certain users access to view Transaction Server log files (error and debug), as these files might contain sensitive information about the user and location of the database.

CAUTION: Implementing security on these files will prevent Server Manager from being able to display the logs.

Business Services Server Security

EnterpriseOne provides authentication security to ensure that published business service users are authenticated in EnterpriseOne. The Business Services Server uses the EnterpriseOne Login Module as the authentication mechanism for authenticating users against the security server.

To set up security for the Business Services Server, see *"Configuring Business Services Server Security" in the JD Edwards EnterpriseOne Tools Business Services Server Reference Guide* . This chapter contains instructions on how to implement security for the Business Services Server, which can run on Oracle WebLogic Server or IBM WebSphere Application Server.

You can configure the Business Services Server with the Secure Sockets Layer (SSL) protocol so that all communication is over HTTPS. See *Configuring SSL for EnterpriseOne Servers*.

Configuring the Business Services Server to User Secure File Transfer Protocol (SFTP) for Media Objects

Oracle recommends using SSH file transfer protocol, otherwise referred to as Secure FTP (SFTP), for media object access as a more secure alternative to FTP. When the Business Services Server is configured to use SFTP for media objects, the Media Object published business service can securely upload, download, and delete media objects. For instructions on how to enable SFTP for media objects on the Business Services Server, see *"Enabling Secure File Transfer Protocol (SFTP) for Media Objects" in the JD Edwards EnterpriseOne Tools Business Services Server Reference Guide* .

Secure Log Files

You should give only certain users access to view business services log files, as these files might contain sensitive information about the user and location of the database.

CAUTION: Implementing security on these files will prevent Server Manager from being able to display the logs.

Oracle BI Publisher Server Security

The Oracle BI Publisher Server and the EnterpriseOne HTML Server must be within the same firewall to have two-way web service and HTTP communication.

To create an interactive BI Publisher report, a user must be able to sign on to both BI Publisher and to the EnterpriseOne database. The connection string for the data source, along with the EnterpriseOne JDBC Driver configuration, specifies the database that BI Publisher will access when creating and running interactive reports. At the time that the JDBC driver is configured, it is highly recommended that you select the Use Proxy Authentication option for the data source. Using proxy authentication assumes that the user IDs in BI Publisher and EnterpriseOne are the same, either by duplication or by using Lightweight Directory Access Protocol (LDAP).

Refer to *"Oracle BI Publisher and JD Edwards EnterpriseOne Security" in the JD Edwards EnterpriseOne Tools BI Publisher for JD Edwards EnterpriseOne Guide* for instructions on how to configure Oracle BI Publisher with EnterpriseOne.

You can configure the BI Publisher Server with the Secure Sockets Layer (SSL) protocol so that all communication is over HTTPS. See *Configuring SSL for EnterpriseOne Servers*.

Additional BI Publisher Server Security Considerations

For EnterpriseOne integrations with BI Publisher, it is important to note the following security-related considerations:

- If Oracle Business Intelligence Enterprise Edition (OBIEE) and BI Publisher are installed on the same server, you have to upload the boilerplate feature and configure permissions for users to access it. See *"Missing Boilerplates in Components Folder in BI Publisher" in the JD Edwards EnterpriseOne Tools One View Administration Guide* for details.
- For an integration with EnterpriseOne Composite Application Framework, if OBIEE is installed on the same server as Oracle BI Publisher, you have to disable iFrame busting. For instructions on how to disable iFrame busting, see *"Disabling iFrame Busting" in the JD Edwards EnterpriseOne Tools Composite Application Framework (CafeOne) User's Guide* .

Application Interface Services (AIS) Server and AIS Client Security

The AIS Server is the communication interface between JD Edwards EnterpriseOne and various AIS Server clients. The AIS Server provides a JSON over REST interface (HTTP), a light-weight interface that enables AIS clients to interact with EnterpriseOne applications and forms. Any client or software language that uses JSON over REST can interface with the AIS Server.

You can configure the AIS Server with the Secure Sockets Layer (SSL) protocol so that all communication is over HTTPS. See *Configuring SSL for EnterpriseOne Servers*.

The AIS Server uses EnterpriseOne authentication to authenticate AIS clients. For a list of authentication methods supported for AIS clients, see *"Understanding AIS Authentication" in the JD Edwards EnterpriseOne Application Interface Services Server Reference Guide* .

Starting with EnterpriseOne Tools 9.2.2.2, an AIS Server requires a configuration with the EnterpriseOne Enterprise Server (Security Server). This configuration ensures that login requests to the AIS Server use the site key on the Enterprise Server for encryption. If not configured, all login requests to the AIS Server will fail. See *"Configuring the AIS Server with an EnterpriseOne Enterprise Server" in the JD Edwards EnterpriseOne Application Interface Services Server Reference Guide* .

Secure Configuration Files

The AIS Server uses these configuration files:

- REST.INI
- JDELOG.PROPERTIES

These files contain sensitive information that should not be available to all users, so you should use operating system security to secure the files.

CAUTION: Implementing security on these files will prevent Server Manager from modifying configuration settings within these files.

Timeout Settings

A timeout interval specifies how long the user's machine can remain idle before the server automatically disconnects the user from the application. Set up a policy for inactive session timeout and set this value accordingly.

By default, the AIS Server timeout setting is 30 minutes. If using an Oracle WebLogic Server with ADF runtime (referred to as an ADF Server), the default timeout setting for the ADF Server is 20 minutes. If you adjust these settings, make sure that the timeout for the ADF Server is less than the timeout for the AIS Server.

For more information, see the following topics in the *JD Edwards EnterpriseOne Tools Server Manager Guide*:

- *Create an Application Interface Services (AIS) Server as a New Managed Instance*
- *Install an Oracle Application Development Framework Server Instance*

  An ADF Server is required to run EnterpriseOne ADF applications and the JD Edwards EnterpriseOne Orchestrator Studio.

Secure Log Files

You should give only certain users access to view AIS Server log files (error and debug), as these files might contain sensitive information.

CAUTION: Implementing security on these files will prevent Server Manager from being able to display the logs.

Connectors Security

Connectors are point-to-point, component-based interoperability models that enable third-party applications and JD Edwards EnterpriseOne to share logic and data. JD Edwards EnterpriseOne connector architecture includes Java, Dynamic Java, and Component Object Model (COM) connectors and provides access to JD Edwards EnterpriseOne business logic and data.

Secure Configuration Files

Java connector and COM connector use configuration files to connect to a JD Edwards EnterpriseOne environment. Secure JDBj.ini, interop.ini and JDELOG.PROPERTIES using operating system security.

CAUTION: Implementing security on these files will prevent Server Manager from modifying configuration settings within these files.

Secure Log Files

You should give only certain users access to view connector log files (error and debug), as these files might contain sensitive information about the user and location of the database.

Refer to the *JD Edwards EnterpriseOne Tools Connectors Guide* for more information about connectors.

CAUTION: : Implementing security on these files will prevent Server Manager from being able to display the logs.

Desktop Security

In the context of EnterpriseOne, a desktop is considered the working environment for end users when accessing EnterpriseOne from a Microsoft Windows client or web browser.

Disable Browser Cache Setting

A browser caches various pages and states in memory to increase performance. It may be necessary to disable these performance features on the browser for security reasons, especially for a kiosk environment.

For information about configuring the browser to disable caching, refer to the *JD Edwards EnterpriseOne Tools HTML Server Reference Guide* for your platform located at:

http://docs.oracle.com/cd/E61420_01/index.htm

Update Browser

Update the browser when new versions are released because they often include new security features. See document 745831.1 (JD Edwards EnterpriseOne Minimum Technical Requirements Reference) on My Oracle Support for more information about EnterpriseOne supported browsers:

https://support.oracle.com/rs?type=doc&id=745831.1

Turn Off Browser Autocomplete Setting

For kiosk machines, turn off the autocomplete setting for the browser. Although desirable for frequently accessed pages, this feature should be disabled for privacy and security reasons. Even for an intranet environment, do not enable the autocomplete setting to store passwords.

Set Policy for Unattended PC Sessions

You should create a corporate policy for handling unattended PC sessions. Users are recommended to use the password-locked screen savers feature on all PCs.

Turn Off Server BSFN Trace for Windows Client

Change the ServerLog setting to 0 in the [DEBUG] section of JDE.INI file so that the Windows client does not request the BSFN server logs from Call Object kernel. Refer to the *JD Edwards EnterpriseOne Tools Server Manager Guide* for more information about this setting.

Framebusting

Framebusting is a way to prevent clickjacking, which occurs when a malicious web site pulls a page originating from another domain into a frame and overlays it with a counterfeit page, allowing only portions of the original, or clickjacked, page (for example, a button) to display. When users click the button, they in fact are clicking a button on the clickjacked page, causing unexpected results.

For example, say your application is a web-based application that resides in DomainA, and a web site in DomainB clickjacks your page by creating a page with an IFrame that points to a page in your web application at DomainA. When the two pages are combined, the page from DomainB covers most of your page in the IFrame, and exposes only a button on your page that deletes all records in your web application. Users, not realizing they are actually in the web application, may click the button and inadvertently delete all records.

Framebusting prevents clickjacking by using the following JavaScript to block the application's pages from running in frames:

```
top.location.href = location.href;
```

In Server Manager, you can configure Security settings for the EnterpriseOne HTML Server to prevent framebusting in EnterpriseOne. The settings include:

- frameBustingForLogin
- frameBustingForE1Menu
- frameBustingForApp

The valid values for each setting are:

- **always**. If the page is in an iframe, the page will take over the whole window.

  > **Note:** Starting with Tools Release 9.2.7.4, **always** is not available for frameBustingForApp.

- **differentDomain**. (Default) If the page is in a iframe and the page and parent window are from different domain, the page will take over the whole window.
- **never**. Even if a page is in a iframe, the page will never take over the whole window.

For more information about the configuration group settings for the EnterpriseOne HTML Server, see the *"EnterpriseOne HTML Server" in the JD Edwards EnterpriseOne Tools Server Manager Guide* .

If you configure your application to use framebusting by setting the parameter to always, then whenever a page tries to run in a frame, the JavaScript code is run to define the page as topmost, and the page is disallowed to run in the frame.

If your application needs to use frames, you can set the parameter value to differentDomain. This setting causes framebusting to occur only if the frame is in a page that originates from a different domain than your application. This is the default setting.

> **Note:** The origin of a page is defined using the domain name, application layer protocol, and in most browsers, TCP port of the HTML document running the script. Pages are considered to originate from the same domain if and only if all these values are exactly the same.

For example, say you have a page named DomainApage1 in your application that uses a frame to include the page DomainApage2. Say the external DomainBpage1 tries to clickjack the page DomainApage1. The result would be the following window hierarchy:

- DomainBpage1

  DomainApage1

  DomainApage2

If the application has framebusting set to be differentDomain, then the framework walks the parent window hierarchy to determine whether any ancestor windows originate from a different domain. Because DoaminBpage1 originates from a different domain, the framebusting JavaScript code will run for the DomainApage1 page, causing it to become the top-level window. And because DomainApage2 originates from the same domain as DomainApage1, it will be allowed to run in the frame.

5 Post-Installation Security Configurations

Post-Installation Security Configurations

This chapter discusses additional security configurations that you should perform immediately after installing JD Edwards EnterpriseOne, as well as the initial security setup for administration applications, tables, and other EnterpriseOne tools.

Change Default EnterpriseOne User Passwords

Following an installation, EnterpriseOne creates default EnterpriseOne user IDs and passwords. You must immediately change the default passwords or disable the user accounts. See *Setting Up User Sign-in Security* for more information.

Change Default Database Installation Passwords

Following an installation, the application database instance might contain default, open schema accounts with default passwords. These accounts and corresponding passwords are well-known, and they should be changed, especially for a database used in a production environment.

See your DBA or the administration guide for your database for help with changing default database passwords.

Change Default EnterpriseOne System User Passwords for the Database

The EnterpriseOne installation process creates various database users with a default password ("Same as User"). When setting up sign-in security for EnterpriseOne users, each user sign-in record must be associated with a database user, also referred to as a system user, to access the database.

You should change these database user passwords after a successful installation or upgrade. After changing a database user's password, you might have to modify configuration files for the Deployment Server and EnterpriseOne Security Server (also known as the Enterprise Server) because these servers use information from the configuration files to connect to the database. See *Default Database User Accounts* in this guide for a list of default database user accounts for JD Edwards EnterpriseOne 9.1.

To use the long DB proxy password during an upgrade and ESU installation, you must have the Security Server on and you must add security overrides for all the data sources related to the upgrade or ESU target environment (Tools Release 9.2.5).

The long DB proxy password is not supported during the Installation Workbench. You can only turn on the password after completing the first Installation Workbench, as you need have the Security Server running.

For instructions on how to update the passwords in the configuration file settings on the Deployment Server and Enterprise Server, see "Working with Database Security" in the JD Edwards EnterpriseOne Applications Installation or Upgrade guide for your platform and database:

http://docs.oracle.com/cd/E61420_01/index.htm

Note: As of Tools Release 9.2.4.3, the Database Proxy User password exists on both Database and JD Edwards EnterpriseOne. This Database Proxy password is used to establish the connection between JD Edwards EnterpriseOne and the Database that contains the EnterpriseOne tables. The JD Edwards EnterpriseOne allows a maximum length of 40 characters for the Database Proxy User Password field. This extension for the password character limit provides consistency with other password systems used in the product.

Note: Even though the long DB proxy password is supported as of Tools Release 9.2.4.3, you must use only the short passwords during the install and upgrade processes.

Enabling the Long DB Proxy Password (Tools Release 9.2.4.3)

To enable the long DB proxy password:

1. Stop all the services that works with the database, for example, the Enterprise Server.
2. Open the Development Client in your Deployment Server and ensure that the Security Server is turned off.
3. Access the Work With System Users (P980001) program (use the fast path to P980001).
4. Select your System User. For example, select JDE.
5. Enter the long DB proxy password in the Password field and in the Password-verify field. The long DB proxy password can have up to 40 characters.
6. Click the OK button.
7. Exit the Development Client.
8. Connect to the database and then change the password to the long DB proxy password for your system user, for example, JDE.
9. Connect to the Server Manager Console and then change the value in the ProxyPassword field to a long DB proxy password in JDE.INI for all the services that work with the database, for example, the Enterprise Server.
10. Turn on the security server again in the Deployment Server.
11. Restart all the services and verify that your environment is working as expected.

Enabling the Short DB Proxy Password (Tools Release 9.2.4.3)

To enable Short DB Proxy password:

1. Stop all the services that works with the database, for example, the Enterprise Server.
2. Open the Development Client in your Deployment Server and ensure that the Security Server is turned off.

3. Access the Work With System Users (P980001) program (use the fast path to P980001).
4. Select your System User. For example, select JDE.
5. Enter the short DB proxy password in the Password field and in the Password-verify field. The short DB proxy password can have up to 10 characters.
6. Click the OK button.
7. Exit the Development Client.
8. Connect to the database and then change the password to short DB proxy password for your system user, for example, JDE.
9. Connect to the Server Manager Console and then change the value in the ProxyPassword field to a short DB proxy password in JDE.INI for all the services that work with the database, for example, the Enterprise Server).
10. Turn on the security server again in the Deployment Server.
11. Restart all the services and verify that your environment is working as expected.

Set Up an Independent Security Environment

Set up a separate environment to design and test security before deploying it to the production environment. When testing, start with the least privileges and add more rights as required.

Applying Security to JD Edwards EnterpriseOne Tools Administration Applications

This section discusses the administration applications, reports, and tables for which you must set up security to limit access to only administrators. It contains the following topics:

- *Limit Access to EnterpriseOne Tools Administration Applications and Reports*
- *Limit Access to JD Edwards EnterpriseOne Administration Tables*
- *Limit Access to Real-Time Events (RTE) Administration Applications*
- *Limit Access to Design Tools and Universal Table Browser*
- *Limit Access to Data Browser*
- *Limit Access to the User Security Application*
- *Set Up Column Security on Work with Submitted Jobs*

You use the EnterpriseOne Security Workbench (P00950) to set up security for the applications, reports, and tables mentioned in this section.

Limit Access to EnterpriseOne Tools Administration Applications and Reports

Use application security in Security Workbench to allow only CNC administrators access, at a minimum, to the following applications and reports:

- Applications under the System Administration Tools menu.
- Applications under the Package and Deployment Tools menu.

- Applications under the System Installation Tools menu.

You can also obtain a list of all JD Edwards EnterpriseOne Tools-related applications by searching in Object Management Workbench (OMW) for H9* system code.

See *Managing Application Security* in this guide.

Limit Access to JD Edwards EnterpriseOne Administration Tables

Use row security in Security Workbench to allow only CNC administrators the ability to insert and modify data, at a minimum, from these system administration tables:

Table Description	Table Name
Security Workbench	F00950
Sign-on security	F98OWSEC
System user security	F98OWPU
OCM	F986101
Data Source Master	F98611
OMW User Roles	F98220
User Profile	F0092
User Preferences	F00921
User-Role Relationship	F95921
Security History	F9813

See *Managing Row Security* in this guide.

Limit Access to Real-Time Events (RTE) Administration Applications

Use application security in Security Workbench to limit access to the following EnterpriseOne applications to administrators only:

- P90701A (Interoperability Event Definition)

- P90702A (Interoperability Event Subscription)
- R90706 (Convert Event Subscriptions) to create Queue Entries

Note: *"Using Guaranteed Events" in the JD Edwards EnterpriseOne Tools Interoperability Guide* for more information.

Limit Access to Design Tools and Universal Table Browser

Use Security Workbench to set up external call security to limit access to Windows-based design tools: FDA.exe, TDA.exe, RDA.exe, and UTBrowse.exe. See *Managing External Calls Security* in this guide.

Limit Access to Data Browser

Use Security Workbench to set up Data Browser security to limit access to the Data Browser application as this can be used to easily access sensitive data from different data sources. See *Managing Data Browser Security* in this guide.

Limit Access to the User Security Application

Use Security Workbench to set up processing option security to limit access to the User Security application (P98OWSEC). EnterpriseOne password policies are managed as processing options for P98OWSEC. See *Managing Processing Option and Data Selection Security* in this guide.

Set Up Column Security on Work with Submitted Jobs

Use Security Workbench to set up column security on the User field of the Submitted Job Search form (W986110BA). When you set up this security, only the user that is logged in and submitted the batch job can view the records in the grid that are a result of the batch job. The user cannot see batch jobs submitted by other users and more importantly, the output from those batch jobs. See *Managing Column Security* in this guide.

Set Up Object Management Workbench (OMW) Security

Administrators should configure roles and allowed actions for an EnterpriseOne developer.

Refer to *Configuring OMW User Roles and Allowed Actions* in this guide for more information on setting up security for OMW users.

Set Up User Sign-In Policies

If you are managing user IDs and passwords in an EnterpriseOne database, Oracle recommends that you set up the following sign-in policies:

- Set up the Password Change Frequency value in the User Security (P98OWSEC) application to ensure that users frequently change their passwords.
- Select the "Force change password for user" option when creating a new user account so that the system will prompt the user to change the password on the next sign-in.
- Limit the number of invalid password attempts (usually three) before a user account is disabled.

See *Setting Up User Sign-in Security* in this guide for more information.

You can set processing options for the User Security (P98OWSEC) application to set up default sign-in policies. Refer to *Setting Processing Options for P98OWSEC* in this guide for more information on setting up password policies.

Enable Auditing of Security Operation

Set the history setting to 1 under the [SECURITY] section of the JDE.INI file on the security server. This setting turns on the auditing for user login and logoff actions. Use the Security History form exit from the Work with User Security application (P98OWSEC) to review this history or audit records regularly according to your organization's security policy.

See *Reviewing User Sign-in Security History* in this guide for more information.

Security Considerations When Using LDAP to Manage Users

If LDAP authentication is enabled in EnterpriseOne, you should securely configure LDAP access from the EnterpriseOne security server by using LDAP over SSL (LDAPS). Refer to *Using LDAP Over SSL/TLS (Release 9.2.1)* in this guide for more information.

Assign Role with Least Privilege for _LDAPDEFLT User

If LDAP authentication is enabled and user-role relationships are being managed in EnterpriseOne, you must set up a default role relationship for the _LDAPDEFLT user. All new users who are synchronized from LDAP to the EnterpriseOne database will be assigned the default user-role relationship. It is recommended that you assign a default role to _LDAPDEFLT user that has least privilege. An administrator can assign or remove other roles using the EnterpriseOne Role Relationships application (P95921) at a later time. See *Modifying the LDAP Default User Profile Settings* in this guide for more information.

Set Up Single Sign-on Node

Change the default node password for _GLOBALNODE even when you are not using single sign-on from Collaborative Portal or Oracle Portal. It is recommended that you set up a unique single sign-on node with a trusted relationship if you are using multiple security servers on different machines in your environment. Refer to *Setting Up JD Edwards EnterpriseOne Single Sign-On* in this guide for more information on setting up single sign-on nodes.

Support of Longer User Names and Passwords

Out of the box, EnterpriseOne does not support more than 10 characters in a user name or password for sign-on. If you want to use more than 10 characters for a user name or password due to compliance issues for web users, you should use one of the following options:

- Enable the Long User and Long Password features in EnterpriseOne to support long user IDs up to 254 characters in length and passwords up to 40 characters in length. For more information, see:

  Setting Up Long User IDs in EnterpriseOne

  Enabling Long Passwords in EnterpriseOne

- Configure Oracle single sign-on or Collaborative Portal single sign-on with EnterpriseOne.

  In this solution, Oracle single sign-on server or Collaborative Portal is responsible for authenticating a longer user name and password. EnterpriseOne uses the single sign-on token to validate the user. You can configure the EnterpriseOne security server to use the same LDAP Server used by the single sign-on server. User mappings from longer user names to EnterpriseOne user names can be provided in LDAP Server. However, in this case, EnterpriseOne non-web users (such as Windows client and Java Connector users) will not be able to log in with more than 10 character user names and passwords. See *Setting Up JD Edwards EnterpriseOne Single Sign-On* for more information.

- Configure Oracle Access Manager single sign-on with EnterpriseOne. (Requires additional license.)

  Using Oracle Access Manager, you can manage long user IDs and passwords in a single sign-on configuration with EnterpriseOne. This configuration does not change the behavior of existing EnterpriseOne user IDs, but it requires mapping EnterpriseOne users to the long IDs. See *Setting Up JD Edwards EnterpriseOne Single Sign-On Through Oracle Access Management 11g Release 2* for more information.

Implement Security for Server Manager After an EnterpriseOne Tools 9.2 Upgrade

JD Edwards EnterpriseOne Server Manager is a web based application that is used to manage the complete life cycle of the JD Edwards EnterpriseOne server products through agents deployed on server machines. Server Manager is delivered with JD Edwards EnterpriseOne Tools.

The Server Manager Management Console communicates with deployed Server Manager agents through a socket connection that uses the Java Management Extension (JMX) protocol.

If you are upgrading Server Manager to EnterpriseOne Tools release 9.2, you must implement additional security for JMX after performing the upgrade. See *"Implement Security for JMX" in the JD Edwards EnterpriseOne Tools Server Manager Guide* .

> **Note:** Implementing security for JMX applies to EnterpriseOne Tools 9.2 upgrades only. A new installation of EnterpriseOne Tools 9.2 automatically includes a JMX security implementation for Server Manager.

Enable Access to EnterpriseOne User Defined Object Security and Administration Applications

In EnterpriseOne, users can create grid formats, queries, EnterpriseOne pages and other types of objects referred to as user defined objects (UDOs). EnterpriseOne provides security and administration applications for managing and authorizing access to user defined objects and features. You must set up security for these applications before setting up security for UDOs. See *Enable Access to UDO Security and Administration Applications* in this guide.

6 Security for Custom Map Viewers

Understanding Security for Custom Map Viewers

Maps used in the JD Edwards EnterpriseOne software, such as the Property Location Map (P15002X), use the Oracle eLocation services (`http://elocation.oracle.com`) to display the most current mapping information. If you need to use a secure connection to send sensitive latitude and longitude information, you must install and configure a custom map viewer instead of using the eLocation service. A custom map viewer enables you to secure the connection, provide options to utilize a different mapping service, and use customized point and data themes.

> **Note:** It is recommended that you use a custom map viewer.

You can download a map viewer from the Oracle Technology Network (`http://www.oracle.com/technetwork/middleware/mapviewer/downloads/index-100641.html`), along with instructions for installing it (*http://www.oracle.com/technetwork/middleware/mapviewer/documentation/index.html*).

After you have a new mapviewer URL, you must modify the property in the *build.properties* file of the container ant script with the new URL, and then rebuild and deploy the *container.ear* file.

7 Managing Data Source Security

Understanding Data Source Security for EnterpriseOne Tables

A JD Edwards EnterpriseOne installation adheres to Oracle's secure-by-default security model by restricting access to EnterpriseOne tables created in the database. During a Platform Pack installation, the installer creates two initial roles (referred to as group profiles on iBMi and groups on UDB) that define access to data source tables. The following table shows the privileges for each role:

Data Source Role	Alter Table	Create Index	Select	Insert	Update	Delete
JDE Admin	X	X	X	X	X	X
JDE User			X	X	X	X

An X denotes the privilege enabled for tables.

> **Note:** During the installation, an administrator can modify the names of these roles in the Platform Pack Installer. Therefore, the names of the roles might not reflect the names in the preceding table. For more information, see "Working with the Platform Pack" in the JD Edwards EnterpriseOne Installation and Upgrade guides, which you can access here: `http://docs.oracle.com/cd/E61420_01/index.htm`

After running the Platform Pack installation and before running the installation workbenches, you must create the equivalent security definitions for the data source in EnterpriseOne. You create these definitions in the Grant Data Source Privileges (P986117) application, which stores the data source security records in the F986117 table. If a database administrator has additional roles defined for the data source, make sure that these roles are defined in P986117 as well.

This security is applied during table creation and pertains only to new tables created anywhere in EnterpriseOne including tables created from Object Management Workbench, an ESU process, table conversions, UBEs for copying tables, and so forth. Security is defined at the data source level and does not impact EnterpriseOne applications security or row security that is defined for users in the Security Workbench.

JD Edwards EnterpriseOne uses only the select, insert, update, and delete privileges defined in the "JDE User" record in P986117. The "JDE Admin" record with the alter table and create index privileges in P986117 is simply used for record keeping and enables access to the database without having to ask the database administrator to create a database role and login credentials.

Although not recommended, you can also disable data source security for a data source. When data source security is disabled, new tables created in the data source have all privileges granted through the *PUBLIC role.

How Data Source Security is Applied in an Install Versus Upgrade

For a **new** EnterpriseOne applications installation, all tables in the data source are secured with the roles specified in the Platform Pack Installer.

For an EnterpriseOne **upgrade**, only tables created by the Platform Pack are secured with the roles specified during the install. Existing business data and control tables are not secured by the install. In the business data and control tables data source, set up roles for a database administrator and database user. Add these same roles to the Grant Data Source Privileges (P986117) application in EnterpriseOne.

Before Performing Table Conversions

Table conversions do not recognize the roles specified in the Platform Pack Installer. Therefore, you must make sure that you add the new roles in P986117 before performing table conversions. The table conversion recreates the table with the new layout, using the security definition you created on the Deployment Server using P986117.

Adding, Reviewing, and Modifying Data Source Security

Use the Grant Data Source Privileges (P986117) application to add, review, and modify security records for EnterpriseOne table access. EnterpriseOne stores these security records in the F986117 table.

To set up data source security records, you must first select the data source in the Data Sources (P986115) application, and then you can set up security for the data source in P986117.

Navigation to P986115: In EnterpriseOne, select the Navigator menu, EnterpriseOne Menus, EnterpriseOne Life Cycle Tools, System Administration Tools, Data Source Management, Database Data Sources.

To add a data source security record to EnterpriseOne:

> **Note:** You must use role (or group) names that exist in the database. This application will not create the roles for you.

1. On Machine Search & Select, select the data source and then click the **Select** button.
2. On Work With Data Sources, click **Find** to load the data source records in the grid.
3. Select the row for the data source and from the **Row** menu, select **Database Privilege**.

   EnterpriseOne displays any existing privileges defined for this data source.
4. On Work With Data Source Privilege, click the **Add** button.

   > **Note:** If there is an existing data source security record, you can create a new record by selecting the existing record, selecting Copy DSrc Records from the Row menu, and then modifying the copied record with a new name and privileges for the new record.
5. On Manage Data Source Privileges, in the Data Source field, enter the name of the data source or click the search button in the field to select a data source.

   After identifying the data source, the Data Source Type field displays the database type of the data source you selected.

6. Make sure that the **Enable Database Security** check box is selected.
7. In an empty row in the grid, add a record for the database administrator role:
   a. In the Data Source Database User / Role column, enter the exact name of the database administrator role defined in the Platform Pack Installer.
   b. In the Type column, enter or select **1** for the Database Administrator type.
   c. Press Tab to see the "Database Administrator" description and default privileges for the record.
8. In the next empty row in the grid, add a record for the database user:
   a. In the Data Source Database User / Role column, enter the exact name of the database user role defined in the Platform Pack Installer.
   b. In the Type column, enter or select **2** for the Database User type.
   c. Press Tab to see the "Database User" description and the default privileges for the record.
9. In the new records, you can adjust the default security according to your security requirements or model by selecting or clearing the check boxes in the following columns:
   - **All Privileges**. Selecting this check box enables all privileges.
   - **Alter Table**
   - **Allow Index**
   - **Allow Select**
   - **Allow Insert**
   - **Allow Update**
   - **Allow Delete**
10. Click the **OK** button to save the records.

To review or modify data source security records:

1. On Machine Search & Select (P986115), select the data source and then click the **Select** button.
2. On Work With Data Sources, click **Find** to load the data source records in the grid.
3. Select a row with the data source and from the **Row** menu, select **Database Privilege**.
4. On Work With Data Source Privilege (P986117), click **Find** to view the current security for the selected data source.

   In the records displayed in the grid, a check mark denotes the privileges granted to each record.
5. To modify a security record, in the appropriate row, click in any column to enable or disable the table privilege. If you enable the "All Privileges" column, then all privileges are granted.

   Remember, the privileges that you define for the role must reflect the privileges for the role in the data source.
6. Click **OK** to save.

   > **Note:** As an alternative method to modify a data source security record, you can select a record and then select **Manage Privilege** from the Row menu.

To disable data source security:

1. On Work With Data Source Privilege, click the **Add** button.
2. On Manage Data Source Privileges, enter the name of the data source or click the search button to browse and select a data source.
3. Clear the **Enable Database Security** check box.
4. On the "Warning Disable Database Security" dialog box, click **OK** to turn off database security.

   Disabling the security grants all privileges to *PUBLIC in EnterpriseOne.

5. Click the **OK** button.

> **Note:** As an alternative method to disable data source security, you can access the security record in the Work With Data Source Privilege form, and then from the **Row** menu, select **Disable Database Security**.

8 Encrypting Sensitive Data in EnterpriseOne

Understanding the Encryption of Sensitive Data in EnterpriseOne

EnterpriseOne uses 128 bit AES encryption for the encryption of certain sensitive data (such as passwords) stored in the database and sensitive data stored in the following EnterpriseOne configuration (INI) files on EnterpriseOne servers:

- jde
- jdbj
- jas
- tokengen
- jdeinterop

A system administrator uses Server Manager to configure the settings in these server configuration files. If a system administrator updates a configuration setting that contains sensitive data such as a password, the encryption system encrypts the data so that it cannot be read by anyone who opens a configuration file manually. See *#unique_149/unique_149_Connect_42_CIHBHBED* for a complete list of INI files and the settings that contain sensitive data.

You can set up encryption before an EnterpriseOne installation using a command line utility program on the Deployment Server. See *Encrypting Sensitive INI File Data Using the Deployment Server*. You can also set up encryption after an installation through Server Manager. Both methods involve using a site key for encryption as described later in this chapter.

> **Note:** Although not recommended, an administrator can still choose to manually access configuration files and edit the passwords in plain text. Regardless, EnterpriseOne can read passwords whether they are encrypted or in plain text.

Sensitive Data in INI Files Managed by Server Manager

The following table contains a list of server INI files settings that are encrypted when entered or updated through Server Manager:

ini File	Server	Settings
jde.ini	Enterprise Server	[SECURITY] Password= [WORKFLOW] WRIPassword= [TRUSTED NODE]

ini File	Server	Settings
		NodePassword=
jas.ini	HTML Server	[OWWEB] FtpPwd= [EVENTS] jndiuser= jndipassword=
jdbj.ini	HTML Server, Transaction Server, and Business Services Server	[JDBj-BOOTSTRAP SESSION] password= [JDBj-SPEC DATA SOURCE] password=
jdeinterop.ini	Transaction Server and Business Services Server	[KEYSTORE] keystorepasswd= certificatepasswd= [TRUST_STORE] truststorepasswd= [MEDIAOBJECT] FtpPwd=
tokengen.ini	HTML Server	[TOKENGEN] NodePwd=

Understanding the Generation of Site Keys for Use with AES Encryption

Starting with EnterpriseOne Tools Release 9.2, the EnterpriseOne encryption system uses a site key to add a higher level of security for sensitive data stored in configuration files and databases. The site key is combined with other values to create an AES key. The encryption system then uses the AES key to encrypt individual data items. Encryption using AES is the industry-standard for achieving a highly secure encryption.

The site key is unique for each customer. A random value is selected for each data item to be encrypted. The site key is combined with the random value and version-based values within the EnterpriseOne system to generate a 128-bit AES key. That AES key is then used to encrypt that data item. With different random values for each data item, it is possible to have up to 16 million different AES keys associated with each site key.

Oracle provides a command line "sitekey" utility program on the Security Server for generating and storing site keys in the JDE.INI file on the Security Server. When sensitive data is entered in Server Manager, Server Manager accesses the site key in the JDE.INI file and uses the site key to encrypt the data item.

Server Manager uses JDENet to retrieve the site key from the main Security Server defined for Server Manager. If the Security Server is not running, Server Manager will retrieve the site key directly from that Security Server's JDE.INI file.

To create a site key value, a system administrator enters a unique password in the sitekey program. The sitekey program generates a site key from this password. The site key program:

- Uses a hashing function to convert the password into a site key value.

  > **Note:** Based on the hashing, it is not possible to recover the password from the site key value.

- Encrypts the site key value and encodes it within a text string.
- Stores the site key text string in the [SITE KEYS] section of the Security Server JDE.INI file. *Example of Site Key Entries in the JDE.INI* shows an example of a text string of a site key value in the SITE KEYS section.

Using site key values for data encryption provides the following benefits:

- Because site key values are generated from unique passwords, it is highly unlikely that two customers will have the same values.
- The encryption and encoding of the site keys use randomized parameters, so multiple text representations of the same site key will almost always be different.
- The site key values are not stored in the program code. Because site keys are stored in the JDE.INI file, each customer has their own site key, which provides a higher level of security.

Site Key Settings in the JDE.INI File

The sitekey program stores a site key in the following settings in the [SITE_KEYS] section of the JDE.INI file:

- **CurrentKey**. This contains the text string of the site key value used to encrypt new data items.
- **PreviousKey**. This contains the text string of the site key value used to decrypt previously encrypted data items; it is never used for the encryption of new data items. If the current site key is changed, the encryption system uses the previous site key to decrypt old data items, after which the new current site key is used to re-encrypt these data items.

Example of Site Key Entries in the JDE.INI shows an example of site key entries in the JDE.INI file.

Example of Site Key Entries in the JDE.INI

```
[SITE_KEYS]

CurrentKey=ADOtRLI/Y93Hhgmx9Me23fCJB5j0/RtMNA+cWtZXtpB6Y2CMJ/
le0dl2ntXiPeIkybDAQievK3Rqj89tVsSac=

PreviousKey=ADk/
sKxVveqYH1gnk8wodNmzNfD07PcQN0K9M4rqqVIBhBDCjsRmATp9m5QU6iYAS1eQJuQmlxrFq2AScnA4c=
```

Changing the Site Key Settings

The purpose of the site key is to provide an encryption system that uses different encryption keys from one customer site to another. Each site key is used to derive a unique set of AES encryption keys. Therefore, there is not a lot of benefit to frequently changing the site key value. When a site key is changed, it requires the decryption and re-encryption of existing encrypted data.

Data is always encrypted using the "CurrentKey" site key. Data will be decrypted using either the "CurrentKey" site key or the "PreviousKey" sitekey, which allows data items to be decrypted using an old site key, and then encrypted using a new site key.

If you change the site key value, all previously encrypted data should be re-encrypted using the new site key value. After you convert all encrypted data using the new site key, then you can use a text editor to manually delete or comment out the "PreviousKey" entry in the JDE.INI.

Only one "PreviousKey" entry is allowed at one time. If at a later time you need to decrypt old data encrypted with the previous site key, you can manually re-add (or uncomment) the "PreviousKey" entry in the JDE.INI. Then the encryption system will decrypt the data and then re-encrypt the data using the "CurrentKey" site key.

Data Encryption for Merged Systems

You might have a scenario in which data from two different EnterpriseOne systems is merged. The data in the combined database might have had different current site keys. The first system can continue to use its current site key. For the second system merged with the first EnterpriseOne system, you must enter its site key text value into the PreviousKey setting in the JDE.INI file of the first system. At that point, the data from both systems can be decrypted. The data from the second system should then have its data re-encrypted using the current site key.

After all the data in the second system is re-encrypted, only the current site key is required for future encryption; the previous site key entry can be manually deleted from the JDE.INI. It cannot be programmatically removed because the programs cannot determine if there is additional data somewhere that is still encrypted with the previous site key.

Prerequisites

Before you can use site keys for encryption, you must:

- Define the EnterpriseOne Security Server name and port in the Server Manager Console. This identifies the JDE.INI file where the site key value resides. Regardless of whether the Security Server is running, the Server Manager agent will retrieve the site key values for the encryption of sensitive data. See *"Specify the JD Edwards EnterpriseOne Server Used for User Authentication" in the JD Edwards EnterpriseOne Tools Server Manager Guide* .
- Ensure that the Security Server is running JD Edwards EnterpriseOne Tools Release 9.2 or higher.

CAUTION: The Security Server must be defined in the Server Manager Console and the SITEKEY must be configured in Security Server jde.ini for the encryption of sensitive data to occur. Otherwise, passwords in the INI files will not be encrypted and will appear as plain text. Also, all servers managed by an instance of Server Manager must use the same site key. For example, if you want to have a production environment with servers that use one site key and a test environment with servers that use a different site key, then you would need to install two separate Server Manager Consoles, one for all servers in the production environment and one for all servers in the test environment.

Setting Up Site Keys on the Security Server

Use the sitekey program on the Security Server to generate a site key value for the Security Server's JDE.INI file.

A site key value is generated from a unique password that you enter in the sitekey program. Entering a unique, strong password ensures that the site key material that is used for the encryption is unique for each customer site. Follow these password rules to create a strong password:

- Enter a minimum of 8 characters and a maximum of 40 characters.
- Include both upper case and lower case letters.
- Include numbers (0, 1, 2, 3, 4, 5, 6, 7, 8, 9).
- Include the special underline (_) character. No other special characters are allowed.
- Use a letter for the first character.
- Use a letter or a number for the last character.
- At a minimum, use two upper case letters, two lower case letters, two numbers, and two special underline characters.

Only one site key is allowed in an EnterpriseOne system. If your system configuration includes more than one Security Server, after you create a site key, you must manually copy the site key text string from the [SITEKEY] section in JDE.INI file to all other JDE.INI files on the other Security Servers.

CAUTION: A site key is cached upon first usage, therefore, you must restart all EnterpriseOne systems to store a new site key in the cache. If you do not refresh the cache, your system could be using two different site keys at the same time, which is problematic because data encrypted with one site key cannot be decrypted with a different site key.

The following tasks describe how to use the commands in the sitekey program. A description of the commands is available in the sitekey program Action Menu:

```
C:\builds\e900\system\bin32>sitekey
        ACTION MENU
 d   Display site key entries found in JDE.INI
 c   Current site key - will prompt for password to be hashed
 p   Previous site key - will prompt for password to be hashed
Enter letter for action to take:
```

To create a current site key value:

1. Launch the sitekey program from the **system/bin32** directory on the Security Server.
2. In the sitekey program, enter **-c** to access the password prompt, for example:

   ```
   $ sitekey -c
   ```

3. At the "Enter Password:" prompt, enter a password for the site key and then press **Enter**.

   The sitekey program converts the password into a site key value that is wrapped, encoded, and converted to a text string that is stored in the [SITEKEY] section in the JDE.INI file.

   It is important to remember this password in case the generated site key text string is accidentally deleted. For more information, see "Recovering Site Key Values."
4. If you have multiple Security Servers, manually copy the site key text string into the JDE.INI files on each Security Server.
5. Restart all EnterpriseOne systems including Enterprise Servers, Server Manager Console, the HTML Server, and other types of servers.

   A site key is cached upon first usage, so you must restart all systems to store a new site key in the cache. To ensure that the new site key is cached in all systems, they should be restarted in the following order:

   a. Security Server (Enterprise Server) configured in Server Manager console.
   b. Server Manager Console.
   c. Other Enterprise Servers.
   d. All other managed instances, including HTML Servers.

   Note: Server Manager agents do not need to be restarted.

To create a previous site key value:

If the current site key is changed, the encryption system uses the previous site key to decrypt old data items so that the new current site key can re-encrypt the date items.

If a new current site key is added, the "current" site key will become the "previous" site key in the JDE.INI settings. If encrypted data is being merged from a system that had used a different site key, then that site key can be added to the JDE.INI by entering its password for the "previous" key. An alternative method would be to copy the site key text from the INI of the merged system, and entering it as a "previous" key directly in the INI.

1. In the sitekey program, enter `-p` to access the password prompt, for example:

   ```
   $ sitekey -p
   ```
2. At the `Enter Password` prompt, enter the password that was used for the former "current" site key, and then press **Enter**.

   The sitekey program converts the password into a site key value that is wrapped, encoded, and converted to a text string that is stored in the `[SITEKEY]` section in the JDE.INI file.
3. Restart all EnterpriseOne systems in the same order as described in the preceding steps for creating a current site key.

To display site key entries stored in the [SITEKEY] section in the JDE.INI file:

In the sitekey program, enter `-d`, for example:

```
$ sitekey -d
```

This confirms that the site key text is in a valid format. It also determines if a current site key and a previous site key came from the same password. Because the site key text uses random numbers for encoding, the text will always be different even for text that stores the same site key value.

Recovering Site Key Values

If a site key value is accidentally deleted from the JDE.INI file, you can recover it by running the sitekey program and entering the same password that you used to create the site key the first time. The hash of the same password will result in the same hash value, which defines the site key value. The site key text string displayed in the [SITE_KEYS] section will look different than the text string of the original site key value because the process uses random values to convert the site key value to a text string.

If you cannot remember the original password for generating the site key, you can recover the site key by opening a service request (SR) through My Oracle Support:

https://support.oracle.com/

In the service request, include the header portion of an encrypted data item. The header portion is the first 14 characters if it is a text encryption, and it is the first 20 hexadecimal digits if it is a binary encryption. Oracle provides you with a new text string version of the site key that you can manually place in the [SITE KEY] section of the JDE.INI file on the Security Server. The new text string contains the site key required to decrypt the given encrypted data item. It will also decrypt all data items that were originally encrypted with the same site key.

As an alternative to entering a service request, if you are using the encryption only for sensitive data in INI files, you can simply enter a new password in the sitekey program to create a new site key. Then in the Server Manager Console, re-enter all password values, and then re-start all EnterpriseOne systems.

CAUTION: This alternate method cannot be used if you have encrypted data stored in the database (such as encrypted data for applications).

Encrypting Sensitive INI File Data Using the Deployment Server

As an alternative to using Server Manager, Oracle provides a command line utility program called E1IniEncrypt for encrypting sensitive data in the INI files. Server Manager is the preferred method for encrypting passwords in the INI files, but E1IniEncrypt may be used during EnterpriseOne Tools release upgrades if Server Manager is not available. See *#unique_149/unique_149_Connect_42_CIHBHBED* for a list of INI data that can be encrypted using E1IniEncrypt.

Oracle recommends running the E1IniEncrypt program on the Deployment Server, but it will run on any EnterpriseOne Windows client machine.

CAUTION: You must have administrative rights on the EnterpriseOne Windows client machine to run this program.

The E1IniEncrypt program is available in the Enterprise Server system for OS platforms.

Oracle recommends running the E1IniEncrypt program on the Deployment Server. It can also be run on any EnterpriseOne Windows client machines or EnterpriseOne Enterprise Server systems that are running on the Windows, Linux, AIX, HPUX, or SOLARIS OS platforms.

You use the following command in the E1IniEncrypt program to encrypt sensitive data in INI files:

```
E1IniEncrypt -<options> <path to ini>
```

Where <options> include:

```
-jde    : Encrypt passwords in JDE.INI
-inter  : Encrypt passwords in JDEINTEROP.INI
-jas    : Encrypt passwords in JAS.INI
-jdbj   : Encrypt passwords in JDBJ.INI
-tok    : Encrypt passwords in TOKENEGEN.INI
```

And where <path to ini> contains the path to the INI file.

The following example command line shows the command for encrypting passwords in a JDE.INI file:

```
E1IniEncrypt -jde C:\tempini
```

The E1IniEncrypt program encrypts the password depending on the type of value in the original password entry:

- If the value is a plain text password, the program encrypts the password. The encrypted value is represented as a text string.
- If the value is an encrypted value from EnterpriseOne Tools 9.1.4 or 9.1.5, then it re-encrypts the value using the latest encryption method (AES encryption with site keys) and then represents the new encrypted value as a text string.
- If the password field contains a value that has already been encrypted using the latest method, it remains unchanged.

Before running E1IniEncrypt, a site key must be set up on the Security Server. See *Setting Up Site Keys on the Security Server* for instructions on how to set up the site key.

To use the E1IniEncrypt program to encrypt sensitive data in an INI file:

1. Locate the INI file, for example the JDE.INI on an Enterprise Server or the jas.ini on the HTML Server, and copy it to a temporary folder on the Deployment Server such as `c:\tempini`.
2. From the JDE.INI of the Security Server, copy the [SITE_KEYS] block with all of its key values into the JDE.INI used by the Deployment Server. The JDE.INI file is typically located at `c:\Windows\JDE.INI`.
3. Use the following command for each INI file to convert the passwords to the latest encryption:

   ```
   E1IniEncrypt -<options> <path to ini>
   ```

   Where <options> include:

   ```
   -jde    : Encrypt passwords in JDE.INI
   -inter  : Encrypt passwords in JDEINTEROP.INI
   -jas    : Encrypt passwords in JAS.INI
   -jdbj   : Encrypt passwords in JDBJ.INI
   -tok    : Encrypt passwords in TOKENEGEN.INI
   ```

   And where <path to ini> is the path to the temporary folder containing the INI files.

4. Check the INI files to verify that the password encryptions succeeded.

   The original passwords in plain text or in EnterpriseOne Tools 9.1.5 format (which begin with "AC") should now be in EnterpriseOne Tools 9.2 format (which begin with "AD"). Any passwords that were already in the EnterpriseOne Tools 9.2 format should remain unchanged.
5. Copy the INI files with the encrypted passwords back to their original locations. For example, copy the JDE.INI back to the Enterprise Server or jas.ini back to the HTML Server.

Encrypting Sensitive INI File Data for the Deployment Server and EnterpriseOne Windows Client Machines

If you are using a site key for the encryption of INI file data in other EnterpriseOne Server configuration files, you can use the same site key to encrypt the password in the following WRIPassword setting in the JDE.INI files used by the Deployment Server and EnterpriseOne Windows clients:

```
[WORKFLOW]
WRIPassword=
```

To encrypt the data in this setting in the JDE.INI on the Deployment Server:

1. Copy the JDE.INI, typically located at **`c:\Windows\JDE.INI`**, into a temporary folder.
2. If the WRIPassword setting is blank, add the plain-text password.
3. From the JDE.INI of the Security Server, copy the [SITE_KEYS] block with all of its key values into the JDE.INI used by the Deployment Server. The JDE.INI file is typically located at **`c:\Windows\JDE.INI`**.
4. Use the following command for each INI file to convert the passwords to the latest encryption:

   ```
   E1IniEncrypt -<options> <path to ini>
   ```

   Where <options> include:

   ```
   -jde    : Encrypt passwords in JDE.INI
   -inter  : Encrypt passwords in JDEINTEROP.INI
   -jas    : Encrypt passwords in JAS.INI
   -jdbj   : Encrypt passwords in JDBJ.INI
   -tok    : Encrypt passwords in TOKENEGEN.INI
   ```

   And where <path to ini> is the path to the temporary folder containing the INI files.
5. Verify that the value in the WRIPassword setting has been encrypted with the Tools 9.2 encryption (which begin with "AD"). The remainder of the JDE.INI should remain unchanged.
6. Copy the JDE.INI from the temporary folder back to its original location.

For the JDE.INI to be used by the EnterpriseOne Windows clients, follow the same steps as above, but copy and convert the JDE.INI located in the Windows client installation folder on the Deployment Server. This installation folder contains the JDE.INI that is used for the installation of new Windows clients.

Encrypting Database Proxy User Passwords (Release 9.2.1)

Starting with EnterpriseOne Tools Release 9.2.1.0, the EnterpriseOne encryption system uses a site key to add a higher level of security for sensitive data stored in a database. Hence, all of the JD Edwards EnterpriseOne database proxy

users added by the Work With System Users program (P980001) will be stored with new encryption scheme in the System User Security table (F98OWPU).

The enhanced encryption scheme is used to store and retrieve database proxy user passwords from the System User Security (F98OWPU) table.

Note: If you have not set up site keys for data encryption, you cannot add new database proxy users.

Encrypting Database Proxy User Password Considerations

- Ensure that Site Key is already configured in the Enterprise Server's JDE.INI file, as Site Key is a prerequisite.
- Because the encryption scheme is AES encryption with site key, you can identify this Encryption Type as 3 and Encryption Type 4 for unknown encryption.
- If ONTHEFLYMIGRATION= true or 1 is set under [Security] section of the Enterprise Server's JDE.INI file, then all the existing database proxy user (encrypted with old scheme such as 3DES or XOR) stored in the System User Security table (F98OWPU) will be converted into AES encryption dynamically.
- If you add a proxy user from Deployment Server, make sure to create the Site Key first and then add this new site key to the local JDE.INI file of the Deployment Server under the [SITE KEY] section as systems without an available Security Server, such as Deployment Server, the site keys are read directly from the local JDE.INI file and not from server's JDE.INI file.

Commands for Encrypting Passwords Used by RUNUBE and RUNUBEXML

When a user uses the RUNUBE command to generate a report on an EnterpriseOne Windows client, the system uses the user ID and password from a text file to access EnterpriseOne and run the report. This user ID and password are in clear text. Oracle recommends that you use a command to encrypt the password in the text file to protect the sensitive information. Use the following RUNUBE command to encrypt the password in the text file the first time you generate a report:

```
runube -Fe <text_file>
```

Any subsequent RUNUBE invocation that uses the text file will use the encrypted password.

RUNUBEXML uses an XML file that contains a user ID and password in clear text. The password in this XML file needs to be encrypted as well, so Oracle provides a command that encrypts the password the first time you run the RUNUBEXML. Any subsequent run of the RUNUBEXML that uses this xml file will use the encrypted password. Use the following command to encrypt the password in the XML file when you generate a report:

```
runubexml E ENCRYPT_V1 <template_file>
```

For more information about the commands that you can use to run reports with RUNUBE or RUNUBEXML, see *"Submitting at the Command Line" in the JD Edwards EnterpriseOne Tools Batch Versions Guide* .

Enhanced Scheduler Password Encryption (Release 9.2.7.3)

With Tools Release 9.2.7.3, JD Edwards EnterpriseOne uses enhanced encryption to store the scheduled job user's password in the Scheduled Job Master table (F91300).

See *Enhanced Scheduler Password Encryption* in the *JD Edwards EnterpriseOne Tools System Administration Guide*

9 Provisioning User and Role Profiles

Understanding User and Role Profiles

Use the User Profile Revisions (P0092) application to add users and set up user profiles. For every user, you must create a user profile, which defines such information as a list of environments that a user can select when signing in to JD Edwards EnterpriseOne and the language preference of the user. You can also assign roles to users. A role defines the tasks that an end user sees in EnterpriseOne.

You can use P0092 to define specific users or roles. This definition includes:

- The role to which a user belongs.

  Roles are an important aspect of EnterpriseOne. By assigning users to roles, system administrators can set user preferences and security records that are based on the roles rather than the individual user. For example, an accounts payable clerk would be part of the AP role.
- The environments that the user can select when signing in to EnterpriseOne.
- The language preference and country code for the text that appears on EnterpriseOne menus, forms, and country-specific applications.

How Using Role Profiles Makes Setting Up User Profiles Easier

Roles eliminate the need to set up preferences for each individual user profile. By assigning individual users to a role, you can assign preferences to the role and have those settings available to all of the individual users who have that role. We recommend creating all role profiles that are needed for the enterprise first. This method makes creating user profiles easier; instead of defining specific environments, packages, and machine configurations for each user, administrators can define them for the role. If an individual in a role needs a different setup, you can assign different setups at the user profile level, which overrides the role settings.

EnterpriseOne uses roles for these purposes:

- Creation of sign-in security records.
- Authorization security, which determines the EnterpriseOne applications and features uses can access.
- Environments.
- User overrides.

Tables Used by the User Profile Revisions Application

The P0092 application uses these tables:

- Library Lists - User (F0092)
- User Display Preferences (F00921)
- User Display Preferences Tag File (F00922)
- User Access Definition (F00925)

- Library List Control (F0093)
- Library List Master File (F0094)
- Anonymous User Access Table (F00926)

Note:

- *"Defining Machines" in the JD Edwards EnterpriseOne Tools Package Management Guide* .
- *Setting Up User Profiles*.
- *Creating and Modifying User and Role Profiles*.
- *Creating Profiles by Using a Batch Process*.

Adding New Users

You can create user profiles one at a time by using the User Profile Revisions (P0092) application, or you can simultaneously create multiple profiles by using batch processes. If you need to add only a small number of individual users, use the User Profile Revisions application.

This section contains checklists of the high-level steps required to add a single new user or multiple new users. These steps do not address third-party setup issues such as assigning network user IDs.

Note: If the Long User feature is enabled, you can use P0092L to set up user profiles with both short and long user IDs. P0092L contains the same features and functionality as P0092. Therefore, the steps for using P0092 in this chapter can also be used when working in P0092L. For information on how to enable the Long User feature, see *Setting Up Long User IDs in EnterpriseOne*.

Adding an Individual User

The following list describes the high-level steps for adding user profiles one at a time.

1. If you plan to create a new role for the user, add an address book record with a valid search type code (for example, **E** for employee).
2. If the existing role profiles are not acceptable for the new user, add a role profile.
3. Add an address book record for the new user.
4. Add a user profile.
5. Add sign-in security records for the user.
6. Use Security Workbench (P00950) to add any security overrides for the user if the user needs different security than the roles to which the user belongs.
7. Populate the machine table for the user's machine.
8. Use User Overrides Revision (P98950) to add any new user overrides for the user if the user needs different user overrides than the role to which the user belongs.

Adding Multiple Users

When you are ready to create user profiles for the first time, you might need to create hundreds of profiles simultaneously. In this case, EnterpriseOne provides batch processes to create the profiles. These batch processes automate the process of user profile creation.

When you decide which role to assign to a user, consider application security as the most important role because:

- Application security has the most extensive setup.
- Managing overrides to the role security is more difficult than, for example, managing overrides to deployment preferences.

  Note: Sign-in security is not based on roles because individuals must have their own passwords. A program exists with sign-in security to quickly create individual security records by role; however, after the records are created, security is assigned by an individual.

The following list describes the high-level steps for adding multiple user profiles simultaneously.

1. Using the Address Book application (P01012), create address book records for roles that you will use in user profiles.
2. Using the User Profile Revisions application, add the role profiles.
3. Populate the various Address Book tables.

   If you are migrating data from a non-JD Edwards EnterpriseOne system, you can populate the data tables with a table conversion. Otherwise, you can manually add data to the Address Book tables.
4. Run the Populate User Profiles (R0092) batch process to create user profile records from existing Address Book records.

   Normally, this report is based on address book records with a search type for employees (**E**).
5. Adjust each user's role assignments.

   Determine the role in which you want to place an individual and manually assign each user to a role. Change the user environments if they are not standard to that role.

   These settings are dictated by role:
   - Environments
   - User Overrides
   - Application Security
6. Run the Summary of Environments, Packages and Profiles batch process (R00921) to view the new user profiles.
7. Use Security Workbench (P00950) to apply application, action, and processing option security for roles and any individual overrides to those roles.
8. Create sign-in security records using the User Security application (P98OWSEC).

   You can create sign-in security records for all individuals within a role by entering one record for the role.
9. Manually populate the F00960 table.

   This table is automatically populated each time a machine signs in to JD Edwards EnterpriseOne. However, if you intend to use schedule packages, you must manually populate this table.
10. Create user overrides for roles.

Normally, you will not create any overrides for individuals because they can easily create their own as they use the software.

Setting Up User Profiles

This section contains the following topics:

- *Understanding User Profile Setup*
- *Creating and Modifying User and Role Profiles*
- *Copying User and Role Profiles*
- *Assigning or Deleting Environments for User and Role Profiles*
- *Assigning Business Preferences to User and Role Profiles*
- *Setting Processing Options for User Profile Revisions (P0092)*
- *Creating Profiles by Using a Batch Process*
- *Reviewing User and Profile Definitions*

Understanding User Profile Setup

Use the User Profile Revisions (P0092) application to set up user profiles. When you set up profiles as a system administrator, you create "group" profiles (using roles) and user profiles for each user in the system. You also determine the environments that are available for each group and user, and set up display preferences, such as language.

Note: If you are setting up user profiles during the installation process, you *must* sign in to the deployment server using the deployment environment. After you have completed the installation process, you can add or modify user profiles from any machine *except* the deployment server.

These steps outline the high-level process for setting up user profiles:

1. Create all of the role profiles for the enterprise.

   See *Setting Up Roles*.
2. Create a user profile for every user.
3. Assign to each role or user these preferences:
   - Environments, to determine the environments that you want to be available to each role or user. Environments are assigned at the role level only.
   - Display preferences, to determine JD Edwards EnterpriseOne display characteristics such as language, date format, and country code.

     The Display preferences are controlled on the User Profile Revisions form.

Creating and Modifying User and Role Profiles

The system administrator needs to create a user profile for every user. The user profile defines certain setup and display features, such as access to Fast Path, language, date format, or country code. The administrator should first create all

of the role profiles that are needed for the enterprise. This action makes creating profiles easier; instead of defining specific environments, packages, and machine configurations to each user, administrators can define them for the role. If an individual in a role needs a different setup, you can assign different setups at the user level, which will override the role settings.

If you select a country code for a user, the menu filtering process displays for that user any special menu selections unique to that country code. For example, if you enter **CA** (Canada), that user would see the Canadian Tax Information application on the appropriate menu, which users without that country code would not see.

> **Note:** If the Long User feature is enabled, you can use P0092L to set up user profiles with both short and long user IDs. P0092L contains the same features and functionality as P0092. Therefore, the steps for using P0092 in this chapter can also be used when working in P0092L. For information on how to enable the Long User feature, see *Setting Up Long User IDs in EnterpriseOne*.

Creating and Modifying User Profiles

In the Fast Path, enter `P0092` to access the User Profiles application.

1. On the Work With User/Role Profiles form, perform one of the following tasks:
   - If you want to create a new user profile, click **Add**.
   - If you want to modify an existing profile, click **Find**, select a user profile in the grid, and then click Select.
2. On the User Profile Revisions form, in the User ID field, enter a user ID for the individual profile.

   If you are modifying a user profile, this field displays the user ID. You cannot type new information in this field when you modify a profile.
3. In the header area of the form, complete the remaining fields:

   Address Number

   A number that identifies an entry in the Address Book system, such as employee, applicant, participant, customer, supplier, tenant, or location.

   WhosWhoLineID

   A value that references the Who's Who Line ID in the Address Book record.

   Batch Job Queue

   The computer waiting line that a particular job passes through. If blank, it defaults to the job queue specified in the user's job description.
4. In the Display Preferences area, complete the following fields and then click **OK**.

   Language

   A user defined code (01/LP) that specifies the language to use on forms and printed reports. Before you specify a language, a code for that language must exist at either the system level or in the user preferences.

   Justification

   An option that determines how text is to be read, left to right or right to left. This option is enabled only when Arabic is selected as the language. For all other languages, the system automatically selects the left to right option.

   Set Accessibility Mode

   An option that enables the JD Edwards EnterpriseOne web client to be accessible through the JAWS screen reader software for visually impaired users. The option is deselected by default when a user profile is created.

   Set Simplified Mode (9.1 Update 5)

An option that enables users to view the EnterpriseOne interface in Standard or Simplified mode. Standard mode is for users who need access to the full range of EnterpriseOne actions. If users are in Standard mode, they are able to view the Navigation bar, the Carousel, the Fast Path (if they have the appropriate permissions), and Breadcrumbs.

Simplified mode is for users who need a scaled-down interface that provides only limited actions in EnterpriseOne. In Simplified mode, users see the Banner Bar, Personalization, Help, Username, Environment, and Sign Out options.

Set Service-only Mode (9.2 Update 6)

This option provides an additional layer of security by allowing the security administrator to designate that an EnterpriseOne user is a service-only user, and therefore is denied access to the EnterpriseOne sign-on page and any direct interactive access to applications while still allowing the user to execute AIS REST services and access to Orchestrator Studio.

Date Format

The format of a date as it is stored in the database.

These date formats are valid: YMD, MDY, DMY, EMD. If you leave this field blank, the system displays dates based on the settings of the operating system on the workstation. With NT, the Regional Settings in the Control Panel control the settings for the operating system of the workstation.

Date Separator Character

The character to use when separating the month, day, and year of a given date. If you enter an asterisk, the system uses a blank for the date separator. If you leave the field blank, the system uses the system value for the date separator.

Decimal Format Character

The number of positions to the right of the decimal that you want to use. If you leave this field blank, the system value is used as the default.

Localization Country Code

A code that identifies a localization country. It is possible to attach specific county functionality that is triggered baed on this code using the country server methodology in the base product.

Universal Time

A code that you use to associate a time zone with a user's profile. This code represent the user's preferred time zone, and it must be a value from the UDC table (H91/TZ).

Time Format

A value that determines the user's preferred format for time-of-day. The user can choose from a 12- or 24-hour clock.

Daylight Savings Rule

The rule name that specifies the daylight savings rule for a region or country.

See *"Creating Daylight Savings Rules" in the JD Edwards EnterpriseOne Tools System Administration Guide* .

Creating and Modifying Role Profiles

In the Fast Path, enter `P0092` to access the User Profiles application.

1. On the Work With User/Role Profiles form, perform one of the following tasks:
   - If you want to create a new role, select **Add Role** from the Form menu.
   - If you want to modify an existing profile, select the **Roles Only** option, click **Find**, select a role in the grid, and then click **Select**.

2. On the Role Revisions form, complete the following fields:

Role
If creating a new role, enter a name for the role, for example PAYROLL, and enter a description for the role in the adjacent field.

You cannot modify this field if you are modifying an existing role.

Address Number
Enter an Address Book number if the role will be used with a workflow.

WhosWhoLineID
A value that references the Who's Who Line ID in the Address Book record.

Batch Job Queue
The computer waiting line that a particular job passes through. If blank, it defaults to the job queue specified in the user's job description.

Sequence Number
A number that specifies the sequence number of the role in relation to other roles. For a user assigned to more than one role, the sequence number determines which role is chosen when a security conflict exists among the different roles.

In the Display Preferences area, complete the remaining fields:

Justification
An option that determines how text is to be read, left to right or right to left. This option is enabled only when Arabic is selected as the language. For all other languages, the system automatically selects the left to right option.

Set Accessibility Mode
An option that enables the JD Edwards EnterpriseOne web client to be accessible through the JAWS screen reader software for visually impaired users. The option is deselected by default when a user profile is created.

Set Simplified Mode (9.1 Update 5)
An option that enables users to view the EnterpriseOne interface in Standard or Simplified mode. Standard mode is for users who need access to the full range of EnterpriseOne actions. If users are in Standard mode, they are able to view the Navigation bar, the Carousel, the Fast Path (if they have the appropriate permissions), and Breadcrumbs.

Simplified mode is for users who need a scaled-down interface that provides only limited actions in EnterpriseOne. In Simplified mode, users see the Banner Bar, Personalization, Help, Username, Environment, and Sign Out options.

Set Service-only Mode (9.2 Update 6)
This option provides an additional layer of security by allowing the security administrator to designate that an EnterpriseOne user is a service-only user, and therefore is denied access to the EnterpriseOne sign-on page

and any direct interactive access to applications while still allowing the user to execute AIS REST services and access to Orchestrator Studio

Date Format

The format of a date as it is stored in the database.

These date formats are valid: YMD, MDY, DMY, EMD. If you leave this field blank, the system displays dates based on the settings of the operating system on the workstation. With NT, the Regional Settings in the Control Panel control the settings for the operating system of the workstation.

Date Separator Character

The character to use when separating the month, day, and year of a given date. If you enter an asterisk, the system uses a blank for the date separator. If you leave the field blank, the system uses the system value for the date separator.

Decimal Format Character

The number of positions to the right of the decimal that you want to use. If you leave this field blank, the system value is used as the default.

Localization Country Code

A code that identifies a localization country. It is possible to attach specific county functionality that is triggered baed on this code using the country server methodology in the base product.

Universal Time

A code that you use to associate a time zone with a user's profile. This code represent the user's preferred time zone, and it must be a value from the UDC table (H91/TZ).

Time Format

A value that determines the user's preferred format for time-of-day. The user can choose from a 12- or 24-hour clock.

Daylight Savings Rule

The rule name that specifies the daylight savings rule for a region or country.

See *"Creating Daylight Savings Rules" in the JD Edwards EnterpriseOne Tools System Administration Guide* .

3. Click OK when you are finished.

Copying User and Role Profiles

You can copy all or part of a user or role profile. When you copy an entire user or role profile (display and environment preferences), you are creating a new user or role profile with the information from another profile. When you copy part of a user profile, you are copying the environment preferences from another profile to an already existing user profile.

In the Fast Path, enter P0092 to access the User Profiles application.

1. On the Work With User/Role Profiles form, select a user or role profile and perform one of the following actions:
   - To copy an entire profile (the display, environment, and deployment preferences), click **Copy**.

     The User Profile Revisions form or Role Revisions form appears depending on if you copied a user or role profile. Because this action creates a new profile, the user or role profile that you create cannot already exist in JD Edwards EnterpriseOne.
   - To copy environment preferences, from the Row menu, select **Copy Environment**.

     The User Environment Revisions form appears. This action copies environment prefaces from one user or role profile to another. The user or role profile that you copy to must already exist.
2. If you copied a user, in the User/Role field on User Profile Revisions, enter a user ID to copy the profile into and modify any other information if necessary.
3. If you copied a role, in the Role field on Role Revisions, enter a role to copy the profile into and modify any other information if necessary.
4. Click **OK**.

Assigning or Deleting Environments for User and Role Profiles

You can assign a list of environments that each user or role can choose from when starting EnterpriseOne. If a user does not have a user profile-specific environment assignment, the user can choose from the environments that are assigned from the user's role each time the user starts EnterpriseOne. You can assign more than one environment from which a user can choose. You can delete environments that are no longer relevant to the user.

> **Note:** If environments are set up at the user level, the user will only be able to log into those environments. Also, the same environments must be added to the user's role. If an environment is not at both the user and role level, the user will not be able to log into that environment playing that role.

In the Fast Path, enter P0092 to access the User Profiles application.

1. On Work With User / Role Profiles, click **Find** and then select a user or role profile.
2. From the Row menu, select **Environments**.

   The User Environment Revisions form appears. This form displays the list of environments available for a particular user or role.
3. To add a new environment, in the last row, enter a number that specifies the order in which the environment is displayed in the Display Seq. field.
4. In the Environment field, click the search button to select an environment.
5. To delete an environment from the list, select the environment and click **Delete**.
6. Click **OK** when you are finished.

Assigning Business Preferences to User and Role Profiles

When setting up profiles, you can assign business preference codes. These codes can be used by a customized workflow process to send messages, update a database, or start an application. You define the codes for the preferences based on industry, business partner, or customer. Then you can create an EnterpriseOne workflow process that is based on whether a specific code resides in the user profile.

For example, you assign the code **CUS** for a customer business preference, and then create a workflow process that begins whenever a user or role profile with the CUS business preference enters a sales order.

In the Fast Path, enter `P0092` to access the User Profiles application.

1. Click **Find**.
2. Select a user or profile, and then click **Select**.
3. On the User Profile Revisions or Role Revisions form, from the Form menu, select **Bus Preferences**.
4. On the Business Preferences form, complete any of these fields and click **OK**:
   - Industry Code

     This field associates the user profile with a specific industry, such as manufacturing.
   - Business Partner Code

     This field associates the user profile with a specific business partner.
   - Customer Code

     This field associates the user profile with a specific customer.

     > **Note:** Click Cancel on the Business Preferences form to cancel the addition of the current business preference.

Assigning Standard, Simplified, and Service-only (Release 9.2 Update 6) Modes to User Profiles

By default, all users and roles are assigned Standard mode. The Simplified mode can be assigned to either specific users or roles. If a user logs into EnterpriseOne using the *ALL role, all roles included in *ALL must be assigned as Simplified mode for the user to be assigned Simplified mode.

You can assign Standard, Simplified, Service-only modes to Users and Roles, Users only, or Roles only. The default mode is Standard.

In the Fast Path, enter `P0092` to access the User Profiles application.

1. Select to search on both Users and Roles, Users Only, or Roles Only.
2. Click **Find**.
3. Select a record or multiple records, and then click **Select**.

   The User Profile Revisions screen displays.
4. In the User mode section, select the **Standard**, **Simplified** or **Service-only** (9.2 Update 6) option to assign the required mode to user profiles that you have selected.
5. Click **Save**.

> **Note:** *Click here to review a recording of this feature.*

Viewing where Simplified and Standard Modes Apply (9.1 Update 5)

To view where Simplified, Standard, and Service-only (9.2 Update 6) modes apply:

In the Fast Path, enter P0092 to access the User Profiles application.

1. From the Form exit, click **User Mode**.
2. In the User/Role field, if it is not already populated, in the User/Role field enter the user or role for which you want to view Standard or Simplified modes.
3. Select **Standard**, **Simplified**, **Service-only** (9.2 Update 6), or **All** to search for corresponding records.
4. Click **Find**.

Setting Processing Options for User Profile Revisions (P0092)

Access the Processing Options form for P0092, which you can access from the Interactive Versions (P983051) application.

1. On the A/B Validation tab, enter 1 to enable Address Book validation.
   When enabled, this processing option validates each new user ID against the Address Book Master (F0101) table upon the creation of a user profiles. Upon creation of a user profile, each new user ID is validated against the F0101 table. As a result, you cannot create a user profile for a user who is not already defined in the F0101 table. We recommend that you enable this setting to ensure that Work Center operates correctly. That application requires valid address book numbers.
2. Enter 0 (or leave blank) to disable Address Book validation.
   When disabled, this processing option allows you to create user profiles for Address Book entries that do not yet exist in the F0101 table.

Creating Profiles by Using a Batch Process

You can use the Populate User Profiles batch application (R0092) to run a batch process that automatically creates user profiles from existing address book records. This process enables you to create hundreds of new user profiles at a time. This process can save time, ensure accuracy between the Address Book and user profile records, and ease the transition of taking EnterpriseOne to production.

You can also use this batch process to assign display and environment preferences to users.

Note: If you need to add just a few users, you should use the User Profile Revisions application.

Prerequisites

Before you complete the tasks in this section:

- Create all of the role profile information by using the User Profile Revisions application.
- Define:
  - Role profiles.
  - Environments that each role can access.

To run the Populate User Profiles (R0092) batch application:

In the Fast Path, enter BV to access the Work With Batch Versions - Available Versions form.

1. Enter R0092 in the Batch Application field and click **Find**.

2. Select the EnterpriseOne default version (XJDE0001) or the equivalent for the installation, and then click **Select**.
3. On the Versions Prompting form, click **Data Selection**, and then click **Submit**.
4. On the Data Selection form, create a logic statement that describes the set of users for which you want to create profiles.

   This form already has a search type of **E** (employees) populated, which assumes that the users are all employees. You might want to narrow this selection by submitting it for only a range of employees.

   After you complete the Data Selection form, the Processing Options form appears.
5. On the Processing Options form, enter:

   - One of these values for option 1:

     Enter `1` to run this report in proof mode, which provides an example of what would happen if you were to run the report in final mode.

     Leave blank to run this report in final mode, which creates the user profiles that you specified and creates a report showing the profiles created.
   - One of these values for option 2 to define the user profile record being created for each user:

     Enter `1` to populate the User ID field with the users' address book numbers plus their initials. Typically, user profiles are created with the users' initials preceding their Address Book number.

     Leave this field blank to use just the address book number.

     Complete these user profile fields for option 2:

     Fast Path

     Language

     Date Format

     Data Separator Character

     Data Format Character

     Country
   - For option 3, enter any additional environments that you want the user to have access to instead of the environments already established for the user's role.

Reviewing User and Profile Definitions

The Summary of Environments, Packages and Profiles report (R00921) enables you to review a list of user and role profile definitions. This report summarizes the environment or environments assigned to a role, lists the users in the role, and notes any additional environments that are assigned specifically to an individual user. EnterpriseOne provides two default versions that enables you to summarize either all roles or only specific roles.

In the Fast Path, enter `BV` to access the Work With Batch Versions - Available Versions form.

1. Enter `R00921` in the Batch Application field and click **Find**.

2. Select a version and click **Select**.
   Default version XJDE0001 creates a report for all group (role) profiles in the enterprise. Default version XJDE0002 creates a report about a specific group (role) profile that you specify.
3. On the Versions Prompting form, click **Data Selection** and click **Submit**.
4. On the Data Selection form, create a logic statement that describes the role profiles that you want to summarize.
5. Click **OK**.

Setting Up Roles

This section contains the following topics:

Understanding User Roles

As part of the system setup, you must define the roles for users in the organization. Roles define the tasks that users see when they work in EnterpriseOne Menus and determine what authority the users have in EnterpriseOne.

After you have defined a role, you can associate users with it and apply security to it to provide the appropriate level of access to EnterpriseOne functions. You can assign more than one user to a role, or you can assign more than one role to a user. To establish a role relationship, you use the Role Relationships application (P95921), which enables you to add, remove, or revise a role relationship for a user. Role relationships are revised by removing an assigned role or by changing the expiration date for an assigned role.

Assigning roles accomplishes these purposes:

- Users see only those tasks and perform only those activities that relate to their jobs.
  For example, a user acting in the role of accounts payable clerk might not need to see all of the tasks that an accounts payable manager would need to see. You can create both of these roles and define a different set of tasks for each one.
- Users can have multiple roles.

Within an organization, a user might have many responsibilities, none of which are defined by a single role. A user who is assigned multiple roles can switch roles according to the work required.

> **Note:** Security for a user is not affected when a user changes a role after signing in to EnterpriseOne; only menu filtering and the display of menu information is affected for that user. The security applied to a user is based on how a user signs in to the system.

- Administrators can set up security based on user roles.

  A user's access to applications, forms, table columns, data sources, and so on is based on one or more roles to which the user is assigned.

> **Note:** EnterpriseOne stores the role descriptions in the F00926 table. If you previously defined roles using the UDC table H95/RL, you can run the Populate Role Descriptions From F0092 report (R89959211) to populate the Anonymous User Access Table with those older role descriptions.

This table summarizes the steps an administrator must perform to set up roles for users:

Administrative Step	Applications Used	Forms Used	Tables Used
Populate the User Profile table with roles that are stored in UDC H95/RL during Roles Phase I.	R89959211, R89959212	Not applicable (NA).	F00926, F0092
Run an application to populate the Role Relationships table.	R8995921	NA.	F0092, F95921
Create roles.	P0092 (User Profile Revisions)	W0092A (User Profile Revisions); Form exit from the Work With User Profiles form (W0092D).	F0092
Sequence the roles.	P0092	W0092L (Work With Role Sequences); Form exit from the Work With User Profiles form.	F00926
Create role relationships that associate users with roles.	P95921 (Role Relationships)	W95921A (Work With Role Relationships).	F95921
Add security to roles.	P00950 (Security Workbench)	Various, depending on type of security to be applied to each role.	F00950

The Portal, Solution Explorer, and EnterpriseOne clients use the role relationships data in the F95921 table (Role Relationships) and various APIs to retrieve data and allow users to have assigned roles.

You use EnterpriseOne to administer defined roles for which you have created role relationship records. You can add large numbers of roles to a single user, and you can add large numbers of users to a single role relationship record. You can also use EnterpriseOne to specify the language that is used for the description of a new role.

After you have created one or more role relationships for a user, you can revise the relationships. Role relationships are revised by removing an assigned role or by changing the expiration date for an assigned role. You can also exclude an assigned role from *ALL or add a role to *ALL that was previously excluded.

In addition, you might want to delegate one or more of the roles to another user if a particular user will be unavailable. When you delegate the role relationship records, you can copy existing records to another user. You cannot add role relationships to another user unless those roles are already assigned to you.

Note:

- *"Applying Roles to a Task" in the JD Edwards EnterpriseOne Tools Solution Explorer Guide* .
- *Setting Up Authorization Security with Security Workbench*.

Understanding Role-to-Role Relationships

You create lists of roles that are subsets of another role. For example, you might create an ADMIN role that includes users with the greatest number of administrative responsibilities and the broadest access to applications in EnterpriseOne. You might also create other roles that include individuals with limited administrative responsibilities and access to fewer applications in EnterpriseOne. If you create a distribution list based on roles, you might want to include on the list all roles with some level of administrative responsibility. Anyone in a role that is part of the distribution list would receive messages sent to the ADMIN role.

You use the Work With Distribution Lists form to add or remove roles from the distribution list as needed. Work With Distribution Lists does not influence how security is applied. It only helps to define workflow e-mail distribution lists.

Understanding the Sign-In Role Chooser

When signing in to EnterpriseOne, if the Role Chooser is enabled, users can use the Role Chooser to select a particular role from a list of valid roles. In the Role Chooser, users can either select a particular role or *ALL. You can limit the freedom that a user has to select roles by disabling the Role Chooser. With the Role Chooser disabled, the user must enter EnterpriseOne with *ALL.

At the JD Edwards EnterpriseOne sign-in form, the user enters a user ID and password. The user must then enter a valid environment and role before entering EnterpriseOne. User roles and assigned environments are dependent on each other. The user can select an environment, which then determines the roles that appear in the Role Chooser; or the user can select a role, which determines the environments that appear in the Environment Chooser.

The option for enabling the Role Chooser is a global setting. When enabled, it applies to all users in the system.

This table summarizes the scenarios that can occur when the user encounters the Environment and Role fields at sign-in on the Microsoft Windows client, and the behavior of EnterpriseOne in each scenario:

Sign-in Scenario	JD Edwards EnterpriseOne Behavior
User enters values in both the Environment and Role fields.	The software validates the role against the environment. If the role is not valid for the chosen environment, the Environment Chooser appears and the user must choose a valid environment for the role.
User enters a value only in the Role field.	The Environment Chooser displays only the valid environments for the chosen role.

Sign-in Scenario	JD Edwards EnterpriseOne Behavior
User enters a value only the Environment field.	The Role Chooser displays only the valid roles for the user and the chosen environment.
User does not enter a value in either the Environment field or the Role field.	The Role Chooser appears, containing the valid roles for the user and the default environment that is defined in the jde.ini file, followed by the Environment Chooser, containing only the valid environments for the chosen role. If you do not enter an environment, the Role Chooser displays the roles that are assigned to the default environment, which is defined in the jde.ini file.

Understanding the Menu Filtering Role Chooser

In P95921, you can select the "Choose role on Menu filtering page" option to give users the ability to filter menus by role in the EnterpriseOne Menus. When enabled, the EnterpriseOne web client displays the Role drop-down menu above the EnterpriseOne Menus. From the Role drop-down menu, users can select *ALL (All My Roles) to view a concatenated list of all the tasks enabled for every role that is included in the *ALL role. Alternatively, users can select a particular role from the Role drop-down menu and the system displays only the tasks enabled for that role in the EnterpriseOne Menus.

The "Choose role on Menu filtering page" option is a global setting. When enabled, it applies to all users in the system.

In order for users to filter menus by role:

- The system administrator must enable the "Choose role on Menu filtering page" option in P95921.
- Users must sign in using *ALL.

Note: If a user signs in to EnterpriseOne using a particular role instead of *ALL, then the system only displays the tasks in the EnterpriseOne Menus for that role; the user cannot select a different role in the EnterpriseOne Menus.

Note:

- *Enabling the Role Chooser*.
- *Understanding User Roles*.

Understanding Workstation Initialization File Parameters

At the JD Edwards EnterpriseOne sign-in, you can select one or more roles, depending on how many are assigned to you. If you select ***ALL,** you enter EnterpriseOne in all of the assigned roles that are flagged as Include in *ALL. Two parameters relate to roles in the workstation jde.ini file. These parameters are defined by the administrator when EnterpriseOne is first configured, so you should not have to perform this task when performing routine administrative tasks. This table shows the parameters, the ini file section in which they are found, and the default settings:

Parameter	Section	Default Setting
`LASTROLE`	`[SIGNON]`	*ALL Defines the role that appears for the user at sign-in.

Parameter	Section	Default Setting
`Default Role`	`[DB SYSTEM SETTINGS]`	*ALL

The LASTROLE parameter value defines the role that appears in the sign-in screen when EnterpriseOne is launched.

Creating and Modifying Roles

In the Fast Path, enter `P0092` to access the User Profiles application.

1. On Work With User / Role Profiles, perform one of these tasks:
   - To create a new role, select **Add Role** from the Form menu.
   - To modify an existing profile, click the **Roles Only** option; click **Find** and select a role in the detail area; and then click **Select**.

     > **Note:** You cannot add a role by clicking the Add button on the toolbar of the Work With User/Role Profiles form.
2. On Role Revisions, in the Role field, enter a name for the role, such as `RECEIVING`, and enter a description for the role in the adjacent field.

   When you modify a role profile, this field displays the name of the role.
3. In the Sequence Number field, enter a number to specify the sequence number of the role in relation to other roles.

   For a user assigned to more than one role, the sequence number determines which role is chosen when a security conflict exists among the different roles.
4. Complete any of the remaining fields, as necessary, and click **OK**.

Migrating Roles

On a client machine, open the Batch Versions application in EnterpriseOne and run these universal batch engines (UBEs) to migrate generic roles into the environments.

Set Up Roles

Run the TC R89959211

Table Conversion (TC) R89959211 takes all of the current roles in the UGRP field in the Library Lists - User table (F0092) and adds a Description record for them in the Anonymous User Access Table (F00926). Both the role and description are populated with the role name (for example, OWTOOL). A sequence number is added to the record in the F00926 table as well. This sequence number begins at 1500 and increments by 5 with each record that is written.

This TC has no processing options.

The performance of this TC is directly dependent upon the number of *GROUP records in the F0092 table. It should finish quickly.

After processing, this TC produces no report. To verify that the table conversion completed, open the Universal Table Browser (UTB) and check the F00926 table for some of the roles that are defined in the F0092 table. For example, check the field USER for **OWTOOL**, the field ROLEDESC for **OWTOOL**, and the field SEQNO for a sequence number that is greater than 1500.

Run the TC R8995921

TC R8995921 takes all of the current user profile records in the F0092 table and inserts a user/role relationship record that is based on the F0092.USER and F0092.UGRP tables. The record that is added to the F95921 table contains the user, role (formerly the group for this user in the F0092 table), and effective and expiration dates. Some of these values are based upon the values in the processing options.

The recommended processing option values are:

- Final/Proof Modes

  It is recommended that the TC be run in proof mode first. This mode inserts records to the F95921 table, but it does not remove the group from the user's profile. After the UBE is successfully run in proof mode, check some of the records in the F95921 table to see if they were added successfully. You can re-run the TC in final mode with the same processing options. A new record is not inserted for the user if the effective date is the same as the previously run TC's effective date, so you only remove the group data from the F0092.UGRP field for that user.

- Effective Date

  The start date of the role relationship. With current users (those in F0092 table), you want to use the date that the TC is run. (When running in final mode, use the date that the TC was run in proof mode to prevent the system from adding a new set of records into the F95921 table.) This field must not be modified within the role relationship record later.

- Expiration Date

  The end date of the role relationship. If this date is left blank, the relationship never expires. The role will expire at the beginning of the day of the date that you enter. With the current users (those in the F0092 table), you should leave this blank so they do not expire from their current group or role.

  This field can be modified within the role relationship record later.

- Included In All

  This flag indicates that the security of this role is applied when the user chooses to enter EnterpriseOne under the role of *ALL. Use this flag if a user is being added to a sensitive role, such as Payroll or PVC. This field can be modified within the role relationship record later.

The performance of this TC directly depends upon how many user records are in the F0092 table. It should finish quickly.

This TC produces no report. To verify that the TC completed in proof mode, open the UTB and check the F95921 table for some of the users who were defined in the F0092 table. See that their old group (F0092.UGRP) is now their Role F95921.RLFRROLE. To verify that the TC has completed in final mode, view the F0092 table through the UTB, and verify that no data is in the UGRP fields.

Sequence the Roles

All roles must be assigned a valid sequence number greater than zero in order for the security associated with the role to be applied correctly. The previous UBE and TCs sequence the roles, but probably not in the desired order. Sequence the roles through the Sequence Roles menu option. This displays all of the current roles in a parent/child tree. Expand the tree and view the current sequence number. You can drag and drop these roles into the desired sequence. You *must* click the exit Set Sequence to commit the roles sequence to the database.

Add Environments

Environments can be added to roles. When a user selects a particular role at sign-in, the environments that are associated with that role appear in the Environment Selection List form. If the user selects *ALL environments, all of the environments that are associated with all of the users roles which have been marked as "included in all" appear in the Environment Selection List form. All environments are validated against the user's pathcode.

Set up the JDE.INI/JAS.INI file

Open the jde.ini file and jas.ini file and verify these settings:

Note: You should not have to add or change these settings.

```
[SECURITY]
DefaultRole=*ALL

[REPLICATION]
DefaultRole=*ALL

[SIGNON]
LastRole=<Users Last Role>
This value is populated when a user signs into JD Edwards EnterpriseOne.

[DB_SYSTEM SETTINGS]
DefaultRole=*ALL
```

Server Executables

Run a PortTest.

Set Up Security

Complete these Universal Batch Engines (UBEs) to set up user security.

Run the UBE R98OWPU

UBE R98OWPU performs a select distinct on the F98OWSEC table to find all unique combinations of Proxy (System) User and Data Source. After these records are found, the UBE inserts this record into the F98OWPU table. The record contains the Proxy User, Data Source, Password, and audit information.

Note: This UBE must be run locally because the business function resides only on the client machine.

This UBE has no processing options.

The performance of this UBE is directly dependant upon how many system users are associated with user records in F98OWSEC table. It should finish quickly.

To verify that the UBE completed successfully, open the UTB and check the F98OWPU table for some of the system users that are in F98OWSEC table.

If you want to change a system user password, you have to change it only once for each system user and not for every record in the F98OWSEC table that contains the system user.

Run the UBE R98OWUP (Optional)

UBE R98OWUP updates the current F98OWSEC table records, based upon the processing options that you select. This UBE can populate these new fields for current users, as their F98OWSEC table records do not contain values for these options:

- Password Change Frequency
- Allowed Sign-in Attempts
- Enable / Disable User
- Daily Password Change Limit
- Force Password Change

Set these procession options:

- Proof or Final

  Indicates whether to run in proof or final mode. Proof mode does not commit records.
- Password Change Frequency

  For a given user, this option determines the maximum number of days before the system requires a password change.
- Allowed Attempts

  The number of times that uses can unsuccessfully attempt to log on before their JD Edwards EnterpriseOne account is disabled.
- Enable/Disable User

  Indicates if the user's account is enabled or disabled. A disabled account is not allowed into JD Edwards EnterpriseOne.
- Daily Password Change Limit

  The number of times that users can change their password in one day. Because the last ten passwords of a user are stored in the BLOB, it is a security hole to allow users to change their password as many times as they want. If users want to keep their current password, they can change it 11 times in one day so that they are not back to the original.
- Force Immediate Password Change

  This option requires users to immediately change their password. You might not want to set this option for all users.

The performance of this UBE is directly dependant upon how many system users are associated with user records in the F98OWSEC table. It should finish quickly.

To verify that the UBE completed successfully, access the User Security application (P98OWSEC), and find a user or role whose record should have changed. Verify that the values are correct.

Sequencing Roles

The Work With Role Sequences form contains all of the roles that you defined and enables you to assign a sequence to the roles. The sequence defines a hierarchy of roles and determines which role is used when a security conflict exists among roles when a user signs in as *ALL.

The EnterpriseOne Windows client and Web client differ as to how they use the role sequence to determine which security record is applied. The Web client only checks the first role in the role sequence to determine the security for an application, form, column, row, and so forth. The Windows client checks all the roles in *ALL for security, but uses the role sequence to determine which role to use when there are duplicate security records.

This is an example of duplicate security records in which the Windows client is forced to use the role hierarchy to determine which security record to apply:

A user signs in as *ALL. The *ALL has two roles associated with it—Role 1 and Role 2.

- Role 1 = Form A is secured; no access allowed.
- Role 2 = Form A is not secured; access allowed.

Because of the conflict in security between these two roles, EnterpriseOne uses the information in the role sequence to determine which role to use for security. If Role 1 was higher in the sequence, then the security for that role is applied.

In this same example, if each of these roles had different security records for the same security type, the system would apply the security as defined by both records. For example, if Role 1 does not allow users to view column A and Role 2 does not allow users to view column B, the user would not be able to view either column on the form.

You can configure the EnterpriseOne Web client to use the same role sequencing functionality as the Windows client. This is recommended if you are migrating from the Windows client to the Web client. To enable this functionality in the Web client, use Server Manager to configure the following setting in the [OWWEB] section of the JAS.INI:

```
userRoleHierarchy=true
```

To sequence roles:

In the Fast Path, enter `P0092` to access the User Profiles application.

1. On the Work With User/Role Profiles form, from the Form menu, select **Role Sequence**.
2. On Work With Role Sequences, select a role from the tree structure and drag it to the point in the sequence that you want.

   > **Note:** The system checks the sequence of roles in descending order.

3. After you have set the order that you want, select **Set Sequences** from the Form menu and click **Close**.
4. If you decide you do not want to change the sequence, select **Close Without Set** from the Form menu and click **Close**.

Adding an Environment to a Role

Use the Work With User/Role Profiles form to assign one or more environments to a role or to change an existing environment for a role. When a user signs in to JD Edwards EnterpriseOne, the Environment Chooser and Role Chooser present each user with a list of valid roles and environments.

In the Fast Path, enter `P0092` to access the User Profiles application.

1. On Work With User / Role Profiles, select the **Roles Only** option and click **Find**.

   > **Note:** The Both Users and Roles option also enables you to perform the same task, although the Roles Only option is the simplest way to add an environment.

2. Select a role from the detail area of the grid, and select **Environments** from the Row menu.
3. On the User Environment Revisions form, in the Display Seq. (display sequence) column, specify the order in which the environments will be presented in the Environment Chooser at JD Edwards EnterpriseOne sign-in.
4. In the Environment column, click the search button to select an environment, and then click **OK**:

   > **Note:** If you want to change an existing environment for a role, enter a new value for the Environment parameter and click **OK**.

Assigning Business Preferences to a Role

In the Fast Path, enter `P0092` to access the User Profiles application.

1. On Work With User / Role Profiles, click **Find**.
2. Select a role, and then click **Select**.
3. On the Role Revisions form, from the Form menu, select **Bus Preferences**.
4. On the Business Preferences form, click the search button in the Industry Code field to associate the role with a specific industry, such as manufacturing.
5. In the Business Partner Code field, click the search button to associate the role with a specific business partner.
6. In the Customer Code field, click the search button to associate the role with a specific customer.

Setting Up a Role Relationship

After you have defined a role, you can associate users with it and apply security to it to provide the appropriate level of access to EnterpriseOne functions. You can assign more than one user to a role, or you can assign more than one role to a user. To establish a role relationship, you use the Role Relationships application (P95921), which enables you to add, remove, or revise a role relationship for a user. Role relationships are revised by removing an assigned role or by changing the expiration date for an assigned role.

In the Fast Path, enter `P95921` to access the Work With Role Relationships form.

1. Complete the User field and click **Find**.

   The system displays the user's assigned roles and the available roles in separate tree controls.
2. Select a role from the Available Roles tree control and click the left arrow button to add it to the list of assigned roles.
3. On the Role Revisions form, enter an effective date if you want an effective date that is different from today's date.

   Today's date is the default value for the Effective Date field. If you do not use the default value, enter a date later than today's date; otherwise the software returns an error message.
4. Enter an expiration date in the Expiration Date field, if one is needed.

   The role will expire at the beginning of the day of the date that you enter. The role will not expire if you do not complete the Expiration Date field.

5. Select the **Include in ALL*** option if you want the role to be one that the user can play if the user enters JD Edwards EnterpriseOne playing all roles, and click **OK**.

   If you do not select the Include in *ALL option, this role will not be part of the active roles when the user enters EnterpriseOne using ***ALL** as his role at sign-in. To activate a role that is not included in *ALL, the user must select that particular role when signing on to the system. The role selected will be the only active role during that session.

Enabling the Role Chooser

To enable the Role Chooser:

1. On Work With Role Relationships (P95921), select **Enable Role Chooser** from the Form menu.
2. To enable users to select a role from a list of assigned roles at sign-in, on the Enable/Disable Role Chooser form, select the **Choose role on Login page** option.

   If you do not select this option, users must enter JD Edwards EnterpriseOne using *ALL.
3. To enable users to filter menus by role in the EnterpriseOne Menus, select the **Choose role on Menu Filtering page** option.

Note: Both the Role Chooser and Menu Filtering Role Chooser options are global settings. When enabled, they apply to all users in the system.

Creating Role-to-Role Relationships

To create role-to-role relationships:

1. On Work With Role Relationships (P95921), from the Form menu, select **Distribution Lists**.
2. On the Work With Distribution Lists form, complete the Role field and click **Find**.
3. To add a role to the distribution list, select a role from the Available Roles tree control and click the left-arrow button.
4. On Role Revisions, complete these fields and click **OK**:
   - Effective date

     Enter an effective date if you want the delegation to occur at a date other than the current date.
   - Expiration date
   - Include in *All

     Select this option if you want the role to be one that the user can use if the user enters EnterpriseOne playing all roles.
5. Select the ***ALL** option if you want the role to be one that the user can play if the user enters JD Edwards EnterpriseOne playing all roles.

   EnterpriseOne adds the role to the Assigned Roles tree control.
6. To remove a role from the distribution list, select a role from the Assigned Roles tree control and click the right-arrow button.

   Note: JD Edwards EnterpriseOne does not currently support multilevel roles.

Delegating Roles

To delegate roles:

1. On Work With Role Relationships (P95921), from the Form menu, select **Roles Delegation**.
2. On the Work With Delegation Relationships form, complete the Delegate field by entering the user ID of the user being delegated to and click **Find**.

   The roles of the user who is delegating appear in the Available Roles tree control. The roles of the user who is being delegated to appear in the Assigned Roles tree control.
3. To delegate a role, select the role from the Available Roles tree control and click the left-arrow button.
4. Complete these fields and click **OK**:
   - Effective date

     Enter an effective date if you want the delegation to occur at a date other than the current date.
   - Expiration date
5. Select the ***ALL** option if you want the role to be one that the user can play if the user enters EnterpriseOne playing all roles.

   EnterpriseOne adds the delegated role to the Assigned Roles tree control on the Work With Delegation Relationships form.

   > **Note:** You can use the right-arrow button in the Work With Delegation Relationships form only to remove a role that you delegated to another user. If you try to remove a role that you did not delegate to the user, the software will display a dialog box notifying you that the action is invalid.

Adding Roles to a User

The Add Roles to User form enables you to copy one or more role relationship records to a single user, which is a particularly useful action if you want the user to play many roles. You can copy as many records as you want at one time.

To add roles to a user:

1. On Work With Role Relationships (P95921), from the Form menu, select **Add Roles to User**.
2. Complete the User ID field and click **Find**.
3. Select the roles that you want to add to the user and click **Select**.

   Hold down the Control key to select more than one role to add.
4. On the Role Revisions form, complete these fields:
   - Effective Date

     Enter a date if you want the effective date to be different from the current date.
   - Expiration Date

     The role will expire at the beginning of the day of the date that you enter.
   - Include in *All

5. Select the ***ALL** option if you want the role to be one that the user can play if the user enters JD Edwards EnterpriseOne playing all roles.
6. Click **OK**.
7. If you are adding more than one role relationship record, complete the Role Revisions form for each record that you are adding.

Adding Users to a Role

To add users to a role:

1. On Work With Role Relationships (P95921), select **Add Users to Roles** from the Form menu.
2. Complete the Role field and click **Find**.
3. Select the users that you want to add to a role and click **Select**.

   Hold down the Control key to select more than one user to add.
4. In the Role Revisions form, complete these fields:
   - Effective Date

     Enter a date if you want the effective date to be different from the current date.
   - Expiration Date
   - Include in *All
5. Select the ***ALL** option if you want the role to be one that the user can play if the user enters JD Edwards EnterpriseOne playing all roles.
6. Click **OK**.
7. If you are adding more than user record, complete the Role Revisions form for each record you are adding.

Copying User Roles

You can copy the role relationship records of one user to another from Role Relationships (P95921). You can either copy and add the records, which means that EnterpriseOne adds the copied records to the user's existing records; or you can copy and replace the records, which means that the copied records replace the user's existing records.

To copy user roles:

1. On Work With Role Relationships (P95921), complete the User field and click **Find**.

   The user's roles appear in the Assigned Roles tree control.
2. Click **Copy**.
3. On the Copy User Roles form, select one of these options:
   - **Copy and Add**
   - **Copy and Replace**
4. Complete the To User field to specify the user to whom you want the records copied.
5. Click **OK**.

Adding a Language Translation to a Role

Using the Language Role Description Revisions form, you can either set up the translation of any role that you have defined, or you can change role descriptions for any language.

If you want to view the descriptions of any role in all the languages into which it is being translated, use the Work With Language Role Description form.

In the Fast Path, enter `P0092` to access the User Profiles application.

1. On Work With User/Role Profiles, select the **Roles Only** option.

   > **Note:** The Both Users and Roles option also enables you to perform this task.

2. Select a role from the detail area of the grid and select **Role Description** from the Row menu.
3. To add a language to a role, click **Add**.
4. On the Language Role Description Revisions form, in the Role field, enter the name of the role to which you want to add a language.
5. In the Language field, click the search button to select a language from the list of supported languages.
6. Enter a description of the role in the Role Description field, and then click **OK**.

10 Setting Up Long User IDs in EnterpriseOne

Setting Up Long User IDs in EnterpriseOne

In EnterpriseOne Tools 9.2, in addition to the feature for enabling long user IDs, Oracle provides an option to use long passwords up to 40 characters in length. The Long User ID and Long Password features are autonomous, that is, you can enable one without enabling the other. For more information about enabling long password support in EnterpriseOne, see "Enabling Long Passwords in EnterpriseOne."

Understanding the Long User Feature

As with releases prior to EnterpriseOne Tools 9.2, out of the box, EnterpriseOne user IDs (referred to as "short" user IDs in this chapter) are limited to a maximum of 10 characters. Starting with EnterpriseOne Tools 9.2, administrators have the OPTION to enable the Long User feature to enable users to sign in to EnterpriseOne with a user ID that has a minimum of six characters and a maximum of 254 characters. This feature provides flexibility to support longer formats such as an email address format.

You enable the Long User feature through the User Profile Revisions Long (P0092L) application. In this same application, you set up user profiles with long user IDs by:

- Adding long user IDs to existing user profiles that contain short user IDs.
- Add new user profiles that contain both short and long user IDs.

A user profile cannot exist with only a long user ID. It must contain both a long user ID and short user ID. Because both user IDs are stored together in the same record in F98OWSEC table, users can use either their short user ID or long user ID to sign in to EnterpriseOne.

If a user cannot remember his or her short user ID, you can configure the Auto Suggest feature to display both the user's short user ID and associated long user ID when the user begins to type a long user ID in any form where there is a User ID field. See *"Setting Up Auto Suggest for the User ID Field" in the JD Edwards EnterpriseOne Tools Runtime Administration Guide* for more information.

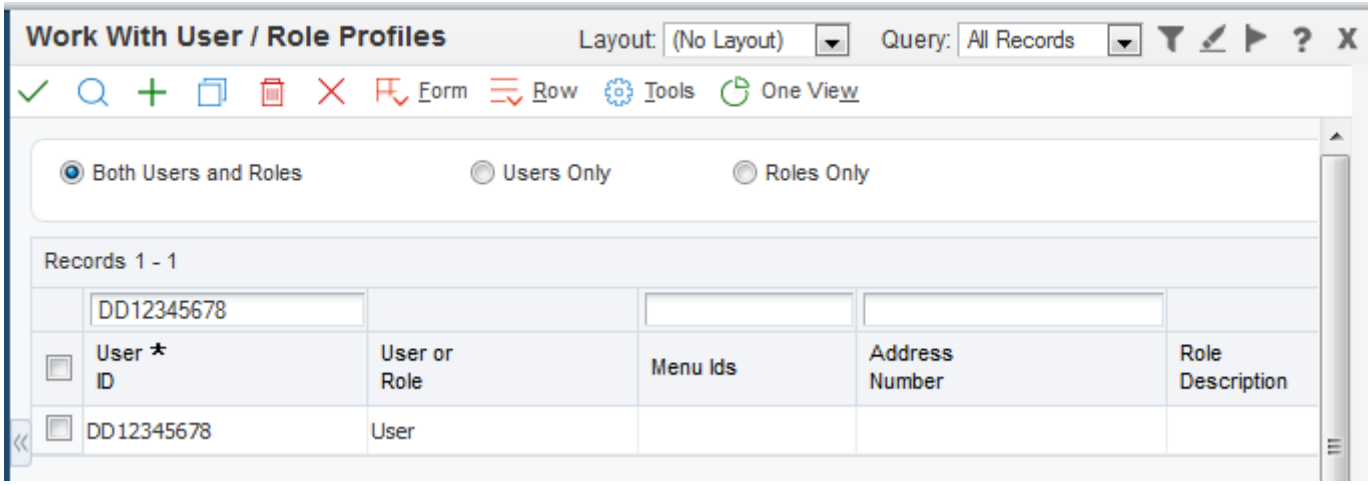
EnterpriseOne also provides the Enable User Migration (P95LUMIG) application to add new long user IDs to existing user profiles in bulk. See *Associating Short User IDs to New Long User IDs in Bulk*

P0092L includes the same features and functionality as the standard User Profile Revisions application (P0092). The only difference is that it provides an additional column for associating a long user ID with the user's short ID. Therefore, after adding long user IDs, you can use P0092L to manage user profiles.

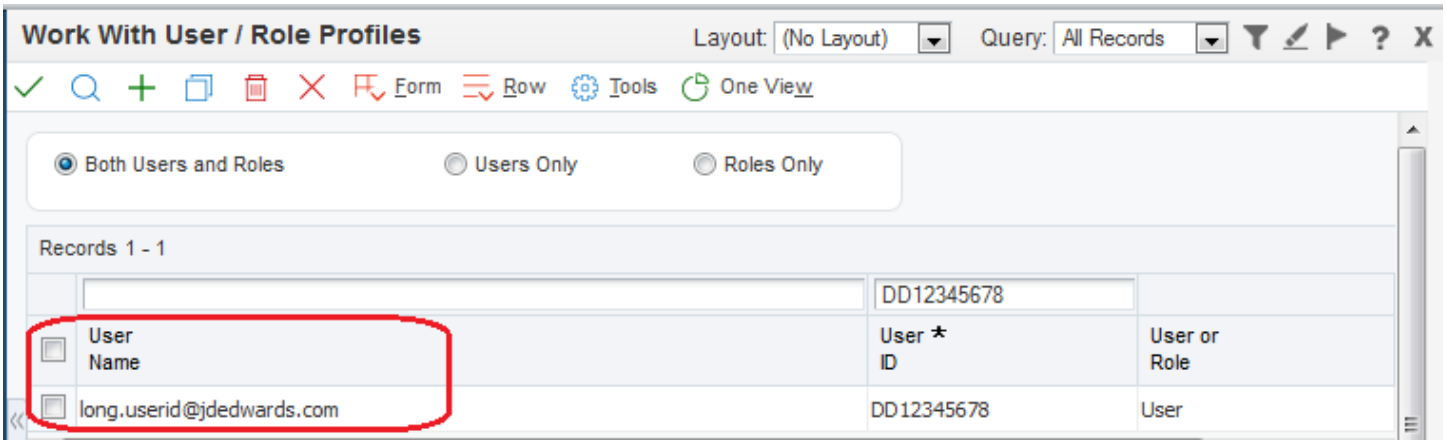
Example: Comparison of P0092 and P0092L shows the difference between P0092 and the P0092L.

Example: Comparison of P0092 and P0092L

The following image shows the DD12345678 user profile in P0092 with the "short" user ID in the User ID column:



The following image shows the DD12345678 user profile in P0092 with the "long" user ID in the User Name column:



Notice that both forms have the same name, "Work With User/Role Profiles", because both forms provide the same features and menus for working with user profiles.

EnterpriseOne Systems and Integrations that Support Long User IDs

When the Long User feature is enabled, most EnterpriseOne systems that require EnterpriseOne credentials for access or for processing will accept long user IDs. This includes but is not limited to the following features and functionality:

- EnterpriseOne web client and EnterpriseOne Windows client.
- Transactions and reports that require a user ID for processing.
- EnterpriseOne auditing features including the auditing of security records and 21 CFR auditing.
- Single sign-on configurations, including single sign-on with Oracle Access Manager (OAM).
- EnterpriseOne configurations with LDAP systems for managing users. An LDAP configuration does require specific settings for supporting long user IDs. See *Enabling LDAP Support in JD Edwards EnterpriseOne* for details.

- Other EnterpriseOne systems or components that requires user credentials for access or processing, such as the Scheduler application, the Configuration Assistant and Change Assistant, RUNUBE and RUNUBEXML, the wizard for developing business services, EnterpriseOne mobile clients and supported tablet clients, and so forth.

Exceptions Where Long User IDs Are Not Supported

Server Manager Console sign-in supports only short user IDs. However, it does support long passwords if the Long Password feature is enabled.

For Collaborative Portal sign-in, long user IDs up to 254 characters in length are not supported. However, if you enabled the Long User feature in EnterpriseOne, you can configure the Collaborative Portal to accept long user IDs up to 200 characters in length. See *Configuring Collaborative Portal to Support "Limited" Long User IDs* for more information.

Considerations for an EnterpriseOne Multiple Foundation Configuration

If you plan to enable both the Long User feature and Long Password feature in a multiple foundation configuration, you must perform additional configuration steps before enabling the Long Password feature. See *Prerequisites for a Multiple Foundation Setup* in this guide.

Enabling the Long User Feature

The Long User feature in EnterpriseOne enables users to sign-in to EnterpriseOne with long user IDs. This setting enables EnterpriseOne systems that require credentials to accept long user IDs. You can create long user IDs before or after you enable the Long User feature.

> **Note:** Once enabled, the Long User feature cannot be disabled. However, if you enable the Long User setting and you decide to not create long user IDs, EnterpriseOne will still accept short user IDs for sign-in credentials.

To enable the Long User feature:

1. Access P0092L.
2. On Work With User/Role Profiles (P0092L), select the **Form** menu, **Enable Long User**.
3. On Enable Long User Feature, select the **Long User ID** check box if it is not already selected, and then click the **Submit** button.
4. In the confirmation dialog box, click **Yes** to continue.
5. Access Server Manager and restart the EnterpriseOne Enterprise Server and the EnterpriseOne HTML Server for the changes to take effect.

Setting Up Long User IDs

In P0092L, you add a new long user ID to an existing user profile that contains only a short user ID. You can do this one-by-one for each user as needed.

You can also use the P95LUMIG application to associate multiple short user IDs to new long user IDs in bulk. See *Associating Short User IDs to New Long User IDs in Bulk* for more information.

Because P0092L contains all of the same features and functionality as P0092, you can also set up new user profiles in this application. Remember that a long user ID cannot exist in EnterpriseOne independently. It must be associated with a short user ID. Therefore, new records in P0092L must contain both a short user ID and a long user ID.

To associate an existing short user ID to a new long user ID:

1. Access P0092L.
2. On Work With User/Role Profiles (P0092L), select the **Form** menu, **Add Long User ID**.
3. On Add Long User ID, in the User ID field, enter the short user ID or click the search button in the field to locate the short user ID.
4. In the User Name field, enter a new long user ID to associate with the short user ID.
5. Click **OK**.
6. To verify that the new long user ID was created, on Work With User/Profiles, enter the short user ID in the User ID field and click the **Find** button.

   EnterpriseOne displays the user profile record with the short user ID in the User ID column and the new long user ID in the User Name column.

Associating Short User IDs to New Long User IDs in Bulk

In P95LUMIG, you can use the grid export and import features to associate existing short user IDs to new long user IDs in bulk. You can also use this process to create new user profiles with a new short user ID and long user ID, which imports the records as new user profiles in P0092L (as well as P0092). Later, you can use P0092L to define other settings for the new user profiles such as language, time format, and so forth.

To associate short user IDs to new long user IDs in bulk:

1. Open a spreadsheet or another excepted file type in which you can use to input short IDs and long user IDs.

   The steps in this section use an Excel spreadsheet. See *"Importing Data from an External Spreadsheet to a Grid" in the JD Edwards EnterpriseOne Tools Foundation Guide* about accepted file types and details about the import and export grid data process.
2. Add two adjacent columns in the table: one for adding short user IDs, and the other for adding a new long user ID for each short user ID, as shown in the following example:

	A	B	C
1		emp2111	employee2111@company.domain
2		emp2211	employee2211@company.domain
3		emp2311	employee2311@company.domain
4		emp2411	employee2411@company.domain
5			

3. Access P95LUMIG.
4. On User Migration Revision (P95LUMIG), select the **Tools** menu, **Import**.
5. On the Import Assistant, click the **Browse** button to locate and select the file that contains the data that you want to import, and then click the **Open** button.
6. On the Import Assistant, depending on the type of file that you are using for the import, complete the appropriate fields to define the data that you are importing. For example, if you are importing the data from the Excel spreadsheet in the preceding example, you would enter the following values:
   - **Starting Cell**: Column = B, Row =1
   - **Ending Cell**: Column = C, Row = 4

7. Click the **Apply** button and then focus on the file to make sure that the data you are importing is highlighted.
8. Click the **Save** button.
9. On User Migration Revision, review and verify the records, and then click the **Select** button.

   After you click Select, EnterpriseOne imports these records as user profile records in the F0092 and F0092L tables.

Managing User Profiles With Long User IDs

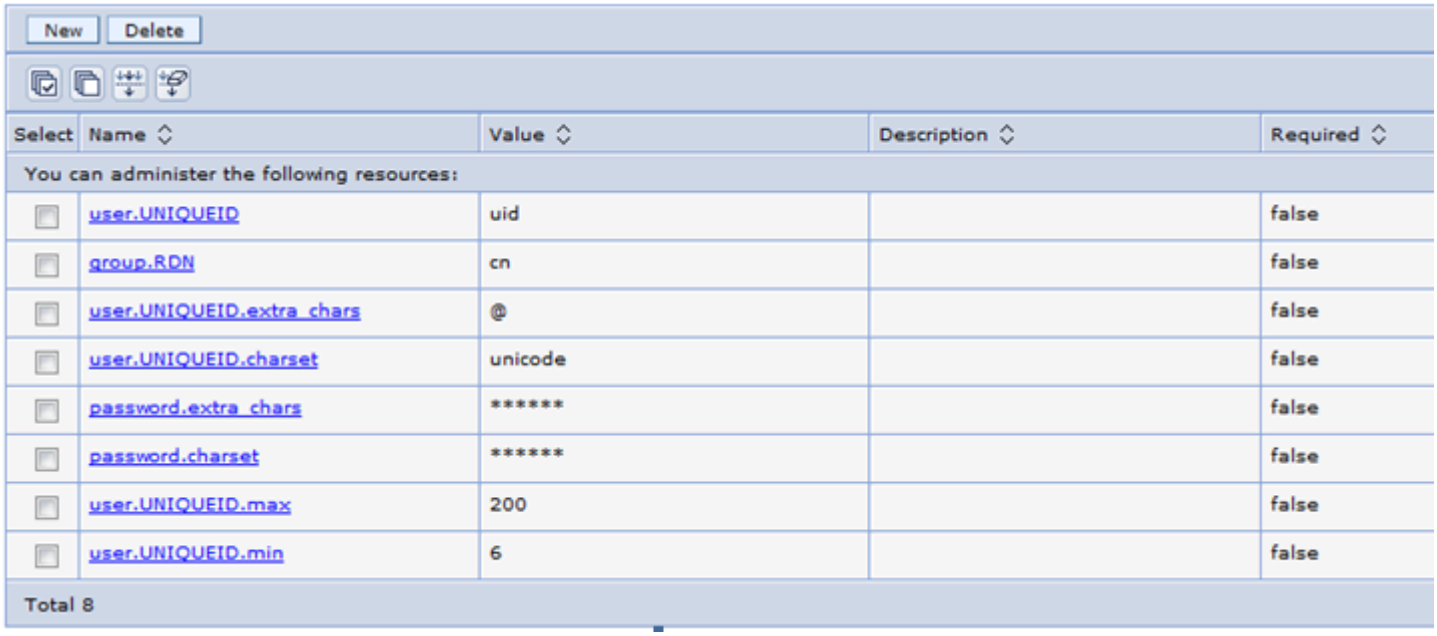
As stated in the "*Understanding the Long User Feature*" section, after enabling the Long User feature and setting up user profiles with long user IDs, you can use P0092L to manage user profiles. P0092L contains all of the same features and functionality as P0092 (Work With User/Role Profiles), the application used to manage user profiles with "short" user IDs. Therefore, when working with user profiles in P0092L, you can follow the steps as described in *Provisioning User and Role Profiles* in this guide.

Configuring Collaborative Portal to Support "Limited" Long User IDs

When the Long User feature is enabled, you can configure Collaborative Portal to support "limited" long user IDs up to 200 characters in length.

To do so:

1. Log in to Portal Integrated Solution Center (Admin Center).
2. Go to Resources, Resource Environment, Resource Environment Providers, WP ValidationService, Custom Properties, New.



New Delete

Select	Name	Value	Description	Required
You can administer the following resources:				
	user.UNIQUEID	uid		false
	group.RDN	cn		false
	user.UNIQUEID.extra_chars	@		false
	user.UNIQUEID.charset	unicode		false
	password.extra_chars	******		false
	password.charset	******		false
	user.UNIQUEID.max	200		false
	user.UNIQUEID.min	6		false
Total 8				

3. In the "Resource environment providers" area, add or edit the following entries:
   - user.UNIQUEID = uid
   - group.RDN = cn
4. Update the following properties for long user validation:
   - user.UNIQUEID.min = 6
   - user.UNIQUEID.max = 200
   - user.UNIQUEID.charset = unicode
   - user.UNIQUEID.extra_chars = @._

     A user id can contain special characters such as:

     .

     @

     _

     If there are some other extra characters allowed, you can append the characters to this property.
5. Update the following properties for password validation:
   - password.charset = unicode
   - password.extra_chars = @._

     A password can contain special characters such as:

     .

     @

     _

     If there are some other extra characters allowed, you can append the characters to this property.
6. Apply these changes and restart the server.

   This enables users with an email address up to 200 characters in length to sign in to the Collaborative Portal.

11 Understanding Sign-in Security

Overview

JD Edwards EnterpriseOne security runs on a logic server in a dedicated internal process. EnterpriseOne uses an encryption algorithm to ensure that applications other than EnterpriseOne cannot access passwords transmitted across the network.You create a security table on the data server that stores information, such as:

EnterpriseOne User
The user ID used to sign in to JD Edwards EnterpriseOne.

EnterpriseOne Password
The user's password, which the software validates when the user signs in to JD Edwards EnterpriseOne.

System User and System Password
The actual user and password used to connect to all database management systems (DBMS). If the JD Edwards EnterpriseOne environment includes more than one DBMS, you can create different system users and passwords for each data source.

Change Frequency
The frequency of password changes required by the software.

Last Change
The date that the password was last changed.

You must define a security record for each user either by group or by individual. It is recommended that you map multiple users to the same system user. For example, each user can use the same system user that the software uses to connect the database management systems. By setting up the security in this manner, you can simplify database administration of users and passwords.

You can also set up unified logon (prior to release 9.2.2 only) with EnterpriseOne to simplify sign-in security. When you set up unified logon, EnterpriseOne uses Windows Authentication to verify security. This verification enables sign-in security to use the network logon information that a user supplies when logging on to Windows; EnterpriseOne does not require the user to enter another user ID and password when signing in.

See *Managing Unified Logon*.

Security Table Access

If you keep the system user and password secure, no users have direct access to the Security table (F98OWSEC). The exception to this situation is for system administrators who maintain the security information. The EnterpriseOne security server has access to the F98OWSEC table through JDENet.

You must perform all of the validation and changes of EnterpriseOne passwords through a JDENet message to the Enterprise Server that has the F980WSEC table. Upon validating an EnterpriseOne password, the JDENet message returns the system user and password that you enter. These words are encrypted across the network. Internally, this system password is used for all connections to databases.

Using the database management system, you should place database security on the F98OWSEC table. You should also assign EnterpriseOne object security to the F98OWSEC table so that users cannot access the object except to enter User Password Revisions.

Password Encryption

You can enter the initial sign-in password for each user in these ways:

- Type it manually.
- Use a default password established through the sign-in security processing options.
- Have EnterpriseOne enter it automatically because the user has an existing security record.

When typing a password manually or when using the processing option default password, you cannot see the password for a new user as you are typing it. When you revise this record, however, the system encrypts the password so that all you see are asterisks. The number of asterisks does not represent the number of characters in the password. The user security application does not know what the password is. The application is given a flag that indicates that a password was entered. The system stores the actual password on the security server within a binary object in the F980WSEC table. The system accesses the binary object when the user security application requests a change or inquiry.

Sign-In Security Setup

This checklist is an overview of the steps that are required to set up sign-in security:

Sign-in Security Setup Step	Description
Determine location of the F98OWSEC table.	Ensure that the F98OWSEC table is located in the system data source on the Enterprise Server, and ensure that the table is mapped to the correct data source through the Object Configuration Manager. If your system data source resides on the enterprise server, the F980WSEC table should reside in the system data source. However, if the system data source is located on the deployment server (or other servers), the F980WSEC table should be moved to the server map data source for the enterprise server. If you have more than one logic server, you should use only one as the security server.
Set database security on the F98OWSEC table.	From within the DBMS, place database security on this table to prevent a user from accessing the object, except to enter passwords through User Password Revisions.
Place security on the logic server's jde.ini file.	The DBMS user ID and password to the Sign On Security table are stored in this file. **Caution:** Implementing jde.ini file security will prevent Server Manager from modifying configuration settings.
Create security records for individual users.	Assign these: • Data source • System user

Sign-in Security Setup Step	Description
	• System password • EnterpriseOne password • User Status • Allowed number of invalid sign-on attempts (optional) • Change frequency (optional) **Note:** If you intend to use a unified logon, every user in the EnterpriseOne security database requires a unique user ID (prior to release 9.2.2 only).
Verify and modify the jde.ini file on the JD Edwards EnterpriseOne logic server for the platform environment.	If you use a unified logon (prior to release 9.2.2 only), you need to change the settings for a unified logon in the [SECURITY] section as well as in the EnterpriseOne [SECURITY] settings.
Set up a unified logon server (prior to release 9.2.2 only).	If you use a unified logon with the JD Edwards EnterpriseOne security, set up a unified logon server for each instance of EnterpriseOne on each server. For example, if you have an NT server with multiple releases of EnterpriseOne, you need a unified logon server for each release on the server. The unified logon server differentiates instances of EnterpriseOne based on the port numbers for these instances. For example, if the port number for EnterpriseOne is 6104, the port number for the associated unified logon server is 6104. Other instances and unified logon servers use different port numbers.
Verify and modify jde.ini file.	Verify and modify the jde.ini file that will be deployed to the server's workstation installations.
Set up sign-in security.	Require sign-in security for all machines.

Process Flow for Standard EnterpriseOne Windows Client Sign-in Security

EnterpriseOne provides sign-in security with an architecture that is designed to provide user security for EnterpriseOne and the logically attached database management systems. The security architecture prevents you from viewing the database or system password and from bypassing EnterpriseOne applications to view and change data.

Standard sign-in security for EnterpriseOne Windows clients uses this process flow:

- Users sign in to EnterpriseOne on their workstations using their user ID and password.

  The workstations can be networked or standalone workstations, laptop computers, or other EnterpriseOne hosts.

  If you enter a valid user ID and password, as validated against the local workstation installation, the start-up process continues.
- As the software starts, it tries to detect an operational network environment.

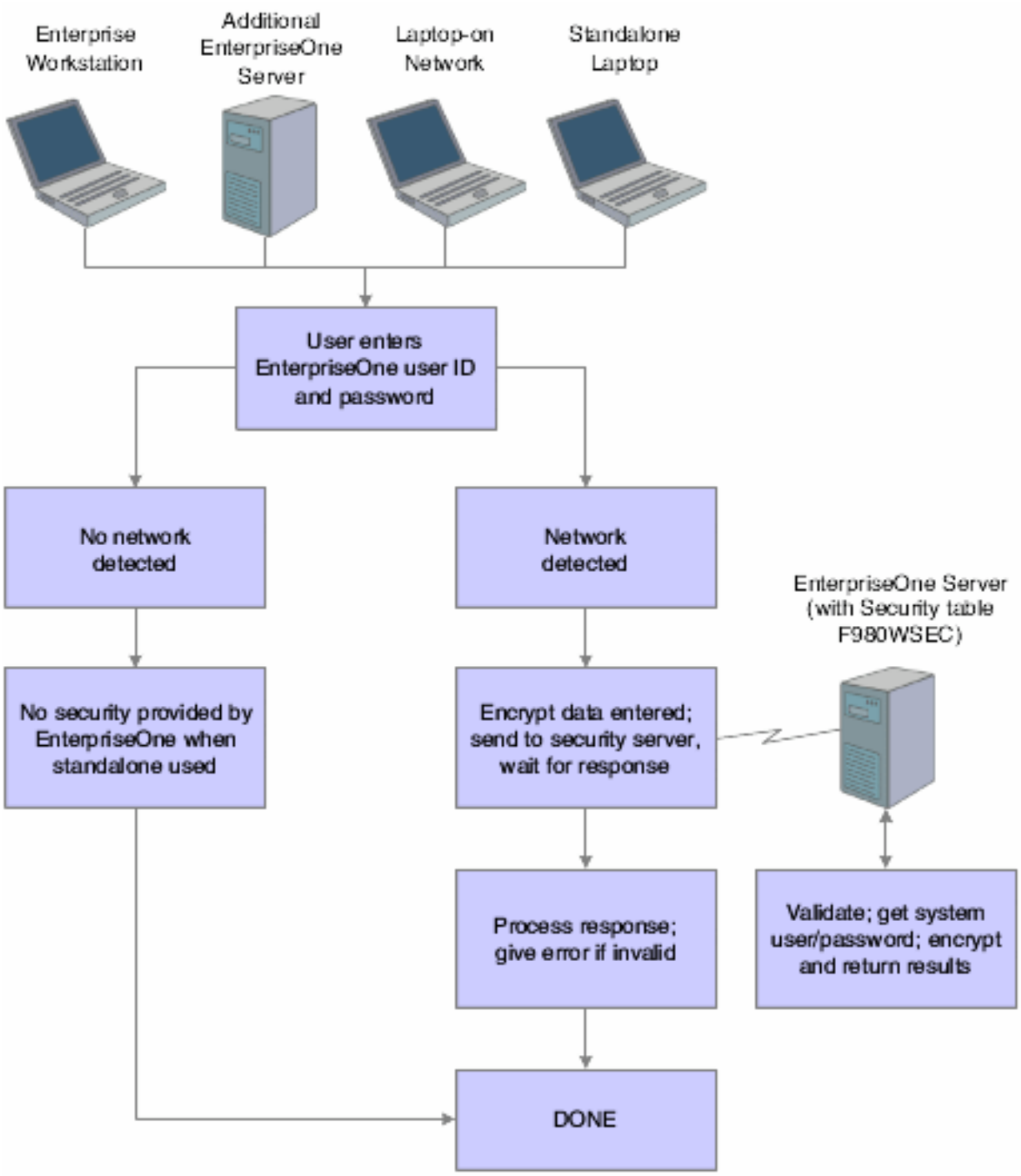
  If a network is not detected, the software allows local operation in a store-and-forward mode. Because the workstation or laptop computer is not connected to a network or an enterprise server, no validation can be

performed against the F980WSEC table. Therefore, security is limited to that provided by the local workstation or laptop installation.

If a network is detected, the software encrypts the password information and sends it over the network to the JD Edwards EnterpriseOne enterprise server.

The enterprise server checks the incoming validation request against a table of valid users and passwords. If the user ID and password information are valid, the software accepts the sign-in values and returns the system ID and password to the logically attached database servers. This information is also encrypted on the enterprise server prior to broadcast on the network.

This graphic displays a process flow model for standard sign-in security:



The process flow for sign-in security with a unified logon (prior to release 9.2.2 only) is as follows:

- A user starts EnterpriseOne on a workstation.
- EnterpriseOne verifies that the unified logon is active and then sends an authentication request to the unified logon server, based on the domain user ID.

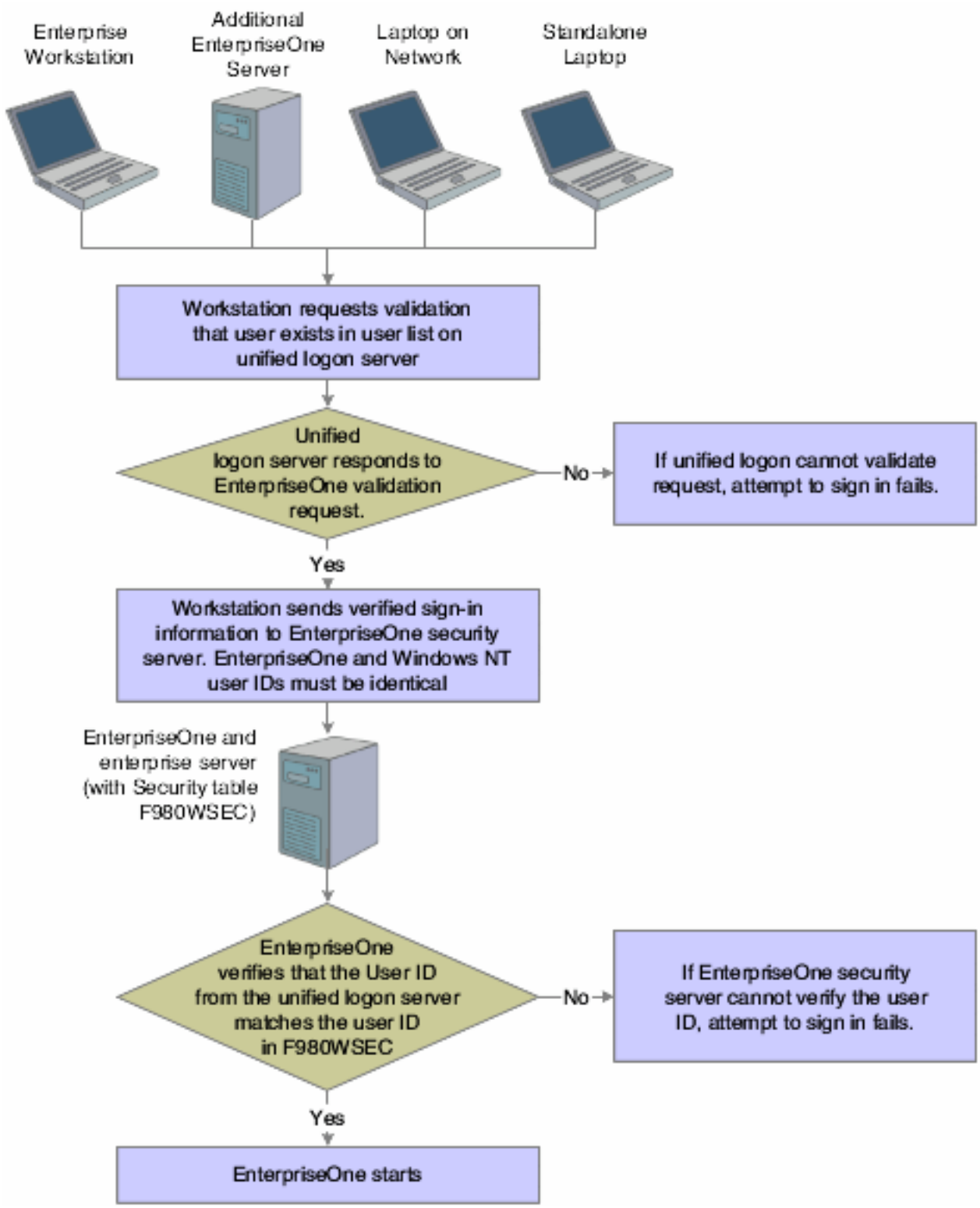
> **Note:** The unified logon server is not a physical server. It is a device that verifies sign-in security against the domain sign-in security maintained by Microsoft Windows.

During jdesnet initialization, jdesnet activates the unified logon server thread. The unified logon server ends automatically when jdesnet ends.

- The unified logon server searches its user list for an entry that matches the domain user ID. When the server finds a match, the server sends a validation request to the enterprise server.
- The Enterprise Server verifies that the response from the unified logon server matches the security information in the F980WSEC table.
- If the security information from the user list on the unified logon server matches the security information in the F98OWSEC table on the enterprise server, the start-up process continues.
- The first time that a user signs in to EnterpriseOne with the unified logon, the Environment Selection appears.

  The user must enter an environment in the Environment field. Select the option to set the environment as the default, and avoid the Environment Selection form on subsequent sign-in attempts.

This illustration displays the process flow for unified logon:


Enterprise Workstation
Additional EnterpriseOne Server
Laptop on Network
Standalone Laptop
Workstation requests validation that user exists in user list on unified logon server
Unified logon server responds to EnterpriseOne validation request.
No
If unified logon cannot validate request, attempt to sign in fails.
Yes
Workstation sends verified sign-in information to EnterpriseOne security server. EnterpriseOne and Windows NT user IDs must be identical
EnterpriseOne and enterprise server (with Security table F980WSEC)
EnterpriseOne verifies that the User ID from the unified logon server matches the user ID in F980WSEC
No
If EnterpriseOne security server cannot verify the user ID, attempt to sign in fails.
Yes
EnterpriseOne starts

ShowUnifiedLogon Setting

The ShowUnifiedLogon setting in the [SECURITY] section of the jde.ini file allows users to reset whether the Environment Selection form appears at sign-in. This feature allows users to change the environment later. This table describes the jde.ini file setting for the [SECURITY] section:

Value	Description
0	A value of 0 for ShowUnifiedLogon disables the Environment Selection form. When you click the option on the Environment Selection form to set a default environment, you set this value to 0.
1	A value of 1 for ShowUnifiedLogon enables the Environment Selection form. When a user signs in to JD Edwards EnterpriseOne, the Environment Selection form appears and allows the user to choose an environment. This setting is the default for ShowUnifiedLogon.

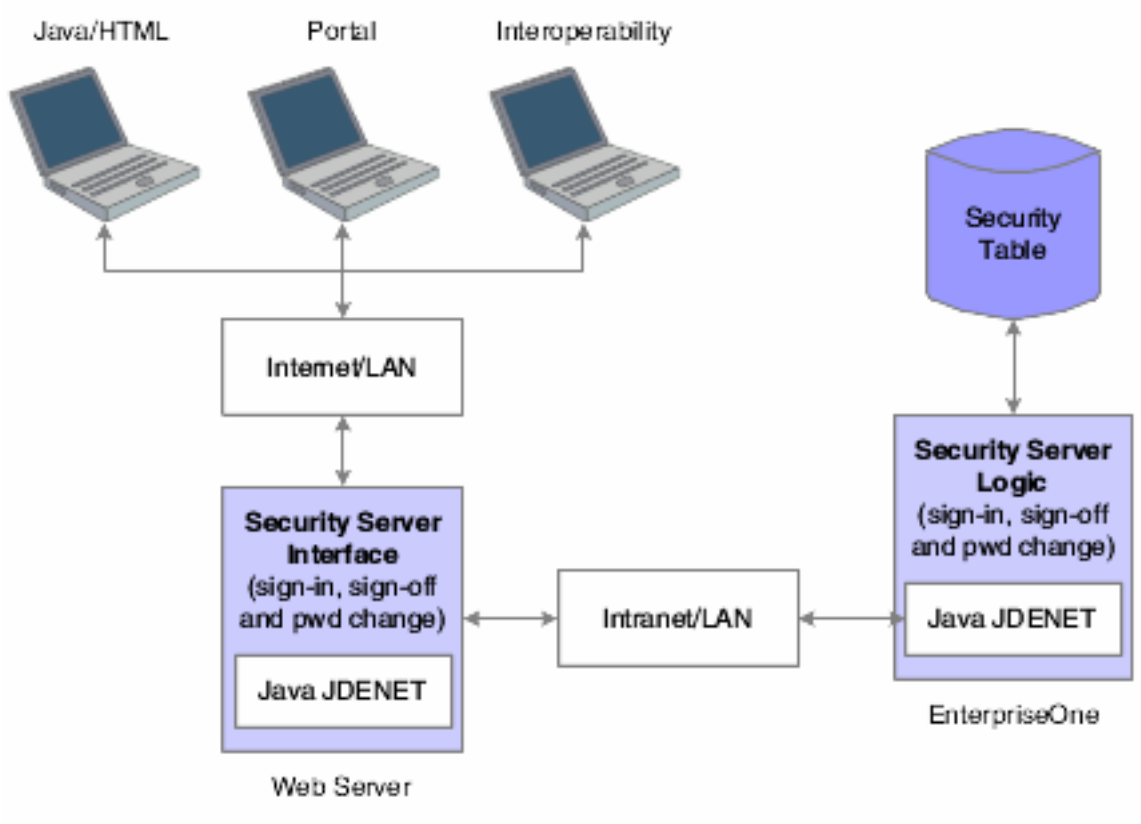
Sign-in Security for Web Users

The EnterpriseOne security server and the F98OWSEC table authenticate Java/HTML, portal, and interoperability users who sign in to JD Edwards EnterpriseOne across the internet to the JAS security server. The JAS security server acts as an interface between the web user's client workstation and the security server.

When web users sign in, disconnect, or make a password change, the HTML server sends the request using a JDENET message to the security server, which, in turn, accesses the F98OWSEC table. The security server then returns the authentication through a JDENET message to the JAS security server. If the user is authenticated, the security info is cached to the JAS security server.

The JAS security server acts as an intermediary between the Java/HTML, Portal, and Interoperability client and the security server.

This graphic displays a process flow for sign-in security with unified logon (prior to release 9.2.2 only) for web users:



As the security intermediary, the JAS security server handles these tasks:

- Connecting to the EnterpriseOne security server for user security authentication and password when a web user signs in.
- Switching to a secondary EnterpriseOne security server when the primary server is down, provided the correct jas.ini settings are defined.
- Notifying Java/HTML, Portal, and Interoperability client workstations when a user password has expired.

  If an Interoperability user's password has expired, sign-in fails without notification of the cause.
- Sending error message to user log after the web user has attempted unsuccessfully to sign in x number of times to EnterpriseOne, where x is the number of sign-in attempts defined in the F98OWSEC table.
- Allowing Java/HTML and Portal users to change name and password.
- Encrypting JDENET messages sent between the JAS security server and the EnterpriseOne security server.
- Keeping a valid user session open until the user signs off or the session expires.

To the web user, sign-in and sign-out function the same as they do to a user on Windows, UNIX, or IBM i platforms.

To set up security for web users through the EnterpriseOne security server, add these parameters to those that already exist in the jas.ini file:

[SECURITY] Parameter in jas.ini File	Parameter Value
NumServers	Total number of EnterpriseOne security servers that are available to web users signing on to the system. If this parameter is missing, the default value is 1 and the primary security server handles the sign-in.

[SECURITY] Parameter in jas.ini File	Parameter Value
SecurityServer	Name of the primary security server.
SecurityServerN	Name of the secondary security server. The value of N is 1 for the first secondary server, 2 for the second, and so on. Assign values to this parameter if you want sign-in to switch to a secondary server if users cannot sign in to the primary server.
UserLogonCookie=	If the value is TRUE, the user can save signon information (username, password, and environment) in an encrypted cookie on the workstation and does not have to type the information in for subsequent sign-ins. If the value is FALSE, the feature is disabled.
#CookieLifeTime unit	Unit of time used to measure a cookie's lifetime. For example, the parameter value day means that the cookie's lifetime is measured in days.
Cookie LifeTime	Amount of time before a cookie expires. The unit of measure is defined by the #CookieLifeTime unit parameter value. If that value is day and the value of the Cookie LifeTime parameter is 7, the cookie expires in seven days.

If you define one primary server and two secondary servers, the jas.ini file [SECURITY] settings look like this example:

```
NumServers=3
SecurityServer=JDED
SecurityServer1=JDEC
SecurityServer2=corowhp2
UserLogonCookie=TRUE
#CookieLifeTime unit is day
CookieLifeTime=7
```

If you define one or more secondary servers, sign-in fails over to the secondary server if the primary server is down. If both the primary EnterpriseOne security server and a secondary server as defined in the jas.ini file fail, the HTML Server fails the user sign-in.

If you do not define a server number or any secondary servers, the jas.ini [SECURITY] settings look like this example:

```
[SECURITY]
SecurityServer=JDED
UseLogonCookie=TRUE
CookieLifeTime unit is day
CookieLifeTime=7
```

Setting Processing Options for P98OWSEC

The User Security application (P98OWSEC) has processing options that you can use to set a default password when creating user security for users or roles, and to set a default change frequency for the password:

Default

Although processing options are set up during the EnterpriseOne implementation, you can change processing options each time that you run an application.

1. Enter a '1' to default the User ID into the password field.

2. Enter in the default Change Frequency.

3. Enter the number of sign-on attempts a user is given prior to being disabled.

4. Enter if a new user is to default to as enabled or disabled.

5. Enter a '1' to force immediate password change of new users.

Password

Although processing options are set up during the EnterpriseOne implementation, you can change processing options each time you run an application.

1. Enter the daily password change limit that will be applied to all users when attempting to change a password.
If this field is 0 or is left blank, there will be no limit on daily password changes.

2. Enter the minimum password length that is to be used when users attempt to change a password.
If this field is 0 or is left blank, the password will not be checked for a minimum length.

3. Enter the minimum number of character that must be used within a password.
If this field is 0 or is left blank, the password will not be checked for characters.

4. Enter the minimum number of numerics that must be used within a password.
If this field is 0 or is left blank, the password will not be checked for numerics.

5. Enter the maximum number of consecutive characters that can be used in a password.
If this field is 0 or is left blank, the password will not be checked for consecutive characters.

6. Enter the minimum number of special characters that must be within a password.
If this field is 0 or is left blank, the password will not be checked for special characters.

12 Setting Up User Sign-in Security

Understanding User Sign-in Security

Use the User Security application (P98OWSEC) to create, test, and change user security for JD Edwards EnterpriseOne and the logically attached database management systems. The security architecture prevents users from viewing the database or system password and from bypassing EnterpriseOne applications to view and change data. EnterpriseOne uses an encryption algorithm to ensure that applications other than EnterpriseOne security cannot access passwords transmitted across the network.

You can also set up a unified logon server for an EnterpriseOne server (prior to release 9.2.2 only). The unified logon server enables EnterpriseOne to use the domain logon information to determine user security. In an EnterpriseOne unified logon scenario, a user needs to enter a user ID and a password only at network logon.

Creating and Revising User Sign-in Security

This section contains the following topics:

Understanding How to Create and Revise User Sign-in Security

A user profile must already exist for a user before you can create user security records for that user. You can create security records one at a time for each of the users, you can set security for a role, or you can set security for all users.

Typically, users within a specific role use similar security information. Oracle recommends that you create a model user with security information that you can copy to create security records for other users. The P98OWSEC application provides a copy function that simplifies the creation of security records.

> **Note:** When you copy security records to a user, security records must not already exist for that user. If you try to copy user security to a user with existing user security records, you will receive an error message.

You should keep user security simple. Managing EnterpriseOne user IDs and system (database) user IDs can become complicated quickly. The simplest way to set up user security is to have all data sources share the same system user ID

and password by leaving the data source field blank when you initially create user security records for users or roles on the Security Revisions form.

When you leave the data source field blank, the P98OWSEC application automatically enters **DEFAULT** in the field. The DEFAULT data source enables you to create one security record for all users. Each time a user accesses a table through an EnterpriseOne application, the software searches for a security record for that user and the specific data source where the table resides. If the software does not find a specific record, then it uses the default data source, which is the security record that you created with the DEFAULT data source field.

You use system user IDs to manage user access to databases. Although you should try to maintain as few system user IDs as you can, occasions arise that require you to set up database security in addition to the EnterpriseOne object and user security for specific users and specific tables. For example, you might need to create system users with additional authority to what the typical system user needs.

Note:

- *"Setting Up Data Sources" in the JD Edwards EnterpriseOne Tools System Administration Guide* .

It is difficult to monitor and administer accounts that are not in use. An administrator should disable these accounts to stop unauthorized access to EnterpriseOne. See *Creating User Sign-in Security* in this section for information on how to disable an account.

Prerequisites

Before you complete the tasks in this section:

- For initial installations of EnterpriseOne, you must set up system user(s) using the Work With System Users (P980001) program to populate the F98OWPU table. You must set up system users before you can add and associate an EnterpriseOne user to a system user using EnterpriseOne Security (P98OWSEC).

  CAUTION: If you attempt to add a user with the P98OWSEC program before you add the system user through the P980001 program, the system may add an invalid record to the F98OWPU table. You might have to delete the invalid record from F98OWPU using the SQL Query tool.

  In the JD Edwards EnterpriseOne Installation and Upgrade Documentation Library, see "Working With Signon Security" in the EnterpriseOne Installation or Upgrade guide that is applicable to your platform and database:

  `http://docs.oracle.com/cd/E61420_01/index.htm`

- Set up all user records in the Address Book application (P01012).
- Create user profiles using the User Profile application (P0092).

  See *Provisioning User and Role Profiles*.

- Attach the proper Address Book record to the user or role profile.
- Review and set the appropriate processing options before using the P98OWSEC application for the first time.

  See *Setting Processing Options for User Profile Revisions (P0092)*.

Forms Used to Create and Revise User Sign-in Security

Note: If the Long Password feature is enabled, EnterpriseOne disables P98OWSEC and redirects you to the P98LPSEC application instead. P98LPSEC contains the same features and functionality as P98OWSEC. Therefore, the steps in this section can be used when working in P98LPSEC. For information on how to enable the Long Password feature, see *Enabling Long Passwords in EnterpriseOne*.

Form Name	FormID	Navigation	Usage
Work With User Security	W98OWSECE	Security Maintenance (GH9052), User Security (P98OWSEC)	Access forms to work with user security.
Security Revisions	W98OWSECB	On the Work With User Security form, click Add.	Create user security.
Copy User Records	W98OWSECN	On the Work With User Security form, select the user or role and click Copy to copy all security records. To copy a single user security record, select the security record from the detail area, and select Copy Record from the Row menu.	Copy user security.
Security Detail Revisions	W98OWSECI	On the Work With User Security form, select the appropriate record, and then select Revise Security from the Row menu.	Revise user and role security.
Administration Password Revisions	W98OWSECF	Security Maintenance menu (GH9052), Administrative Password Revisions (P98OWSEC)	Change a sign-in password.
Sign On Security - Required/Not Required	W98OWSECG	On the Work With User Security form, select Req / Not Req from the Form menu.	Require all machines to use JD Edwards EnterpriseOne sign-in security.

Creating User Sign-in Security

Access the Work with User Security form.

1. Click **Add**.
2. On the Security Revisions form, complete one of these fields:
   - **User ID**

     If you enter a user ID that already exists, you can modify data source information for the user. The system disables all other fields and options for the user ID.
   - **Role**

     If you enter a role that already exists, you will overwrite the security record for role when you enter information on the form.

     > **Note:** When you type information in one of these fields, the system disables the other field. For example, if you type **ROLE1** in the User Class/Role field, the User ID field becomes unavailable for data entry.
3. Complete these fields:
   - **Data Source**

     If you leave this field blank, you will set security for all data sources. **DEFAULT** appears in the Data Source field when you tab out of the field.
   - **System User**
   - **Password**

     We recommend you complete at least the System User field.

     If you create records by role or for all users at one time, the Password field is populated according to the processing option that you select.
4. In the User Status area, select one of these options:
   - **Enabled**

     With User Status enabled, security allows the user to sign in. This option is the default setting when you create user security.
   - **Disabled**

     With User Status disabled, security prohibits the user from signing in to the software.

     > **Note:** If a user commits a security violation, such as exceeding the maximum number of allowed password attempts, the software automatically sets the value for User Status to **Disabled.** The system administrator must access the user security record for the user and set User Status to **Enabled** before the user can sign in. In addition, the system administrator can access Administrative Password Revisions to reset the password of the user, which also restores a user profile to the status of enabled.
5. If you want to set limits on the passwords for users, complete these fields:
   - **Allowed Password Attempts**

Enter the number of invalid password attempts allowed before the system disables access for the user.

- **Password Change Frequency**

  Enter the number of days until the system requires the user to change the password.

- **Daily Password Change Limit**

  Enter the allowed number of times a user can change a password in a day.

- **Force Immediate Password Change**

  Click this check box to require the user to change the password on the next sign-in.

6. Click **OK** to save the current user security information.

Copying User Sign-in Security

A user profile must already exist for a user before you can create user security records for that user. In addition, when you copy security records to a user, security records must not already exist for that user. If you try to copy user security to a user with existing user security records, you will receive an error message.

> **Note:** You should create a model user with security information that you can copy to create other users. Typically, users within a specific role use similar security information.

Access the Work With User Security form.

To copy user security:

1. On the Work With User Security form, find the user, and then perform one of these actions:
   - To copy all user security records for a user or role, select the user or role in the tree structure, and click **Copy**.
   - To copy a single user security record for a user or role, select the security record row in the detail area, and select **Copy Record** from the Row menu.
2. On the Copy User Records form, enter a valid user ID in the To User / Role field and click **OK**.

Revising User and Role Sign-in Security

Access the Work With User Security form.

1. On the Work With User Security form, complete the User ID / Role field.
2. Click **Find**.
3. Select the appropriate record in the tree structure, and then select **Revise Security** from the Row menu.

4. On the Security Detail Revisions form, complete these fields, as necessary:
   - User Status

     Under User Status, you can enable or disable a user profile.
   - Password Change Frequency
   - Allowed Password Attempts

     Note: For a role, select the appropriate option from the Change box to enable each field.
5. Click **OK**.

Revising All User Sign-in Security

Access the Work With User Security form.

1. From the Form menu, select **Revise All**.
2. On the Security Detail Revisions form, in the Change box, select any of these options to enable the related field:
   - User Status
   - Frequency
   - Attempts
   - Change Limit
3. Complete any of these fields, and then click **OK**:
   - User Status

     This field enables you to enable or disable user profiles.
   - Password Change Frequency
   - Allowed Password Attempts
   - Force Immediate Password Change

     This field requires the user to change the password on the next sign-in.

Changing a Sign-in Password

Access the Administration Password Revisions form.

Note: You can also access Administrative Password Revisions from the User Security application. On the Work with User Security form, find the user, select the user in the tree structure, and then select Password Revisions from the Row menu.

User ID
Enter the user ID that you want to force a password change during sign-in. The user ID is the default value in this field when the user record is highlighted and Password Revision is activated.

New Password

Enter a new password. On this form, the system does not restrict the password choices. Any password is valid.

New Password - Verify
Enter the password again to verify it.

Force Immediate Password Change
Select this option to force the user to change the password during the next sign-in.

Requiring Sign-in Security

Use this feature to require all machines to use EnterpriseOne sign-in security. This procedure enables mandatory security only for the environment that you are signed into when you make this change.

Access the Work With User Security form.

1. Select **Req / Not Req** from the Form menu.
2. On the Sign On Security - Required/Not Required form, click the lock icon to change the Security Server to **Required** or **Not Required.**

> **Note:** If you set up the security as **Not Required** and have security turned on through the jde.ini file on the enterprise server, users that comment out signon security in their jde.ini files will still not be able to access any data sources without knowing the system user ID and password. When attempting to access a table in a secured data source, users will receive a database password entry form. If system user IDs and passwords are confidential, no one will be able to access the secured tables.

Enabling Self-Service on System Password Reset (Release 9.2.7)

Use the Work With User Security application (P98LPSEC) to enable the self-service on the reset of the JDE system password. By default, the security architecture prevents users from resetting their password, and they need to seek help from the administrator for resetting their password. You can change the security settings to allow the users to reset their password on an as-need basis.

When the Reset Password feature is enabled and the email ID is set up for the users in their Who's Who, they get an email with a link to reset the password. The link is active for the time specified in the Work With User Security application. When they click the link within that time, they are redirected to the JD Edwards Sign In page with the option to reset their password enabled. The users can use this to reset their password and they can do it as many times as needed.

> **Note:** The self-service of password reset is available for Tools Release 9.2.7 and higher.

> **Note:** *Click here to view a recording of this feature.*

Prerequisites for Password Reset Self-Service

Before you complete the tasks in this section:

- Use the Address Book Revisions program (P0092L) to map each user for whom you want to enable self-service on password reset to a valid Address Book record. Then, enter a valid Email ID for the corresponding Address Book record using the Who's Who program (P01012).
- SMTP server should be configured with a working workflow email setup.

Forms Used to Enable Self-Service on Password Reset

Form Name	FormID	Navigation	Usage
Work With User Security	W98LPSECM	Enter P98LPSEC in the Fast Path field.	Access form to define password reset rules.
Security Detail Revisions	W98LPSECQ	Select Revise All from the Form menu on the Work With User Security form.	Enable password reset self-service and define password reset rules.

Enabling System Password Reset Self-Service

Access the Work With User Security form.

1. On the Work With User Security form, select Revise All from the Form menu.
2. On the Security Detail Revisions form, select the Frequency checkbox and enter a value in the Password Change Frequency field to specify the number of days after which the password will expire.

> **Note:** You can set the password frequency for individual users. To specify a frequency other than the one specified for all users, enter a user ID on the Work With User Security form and select Revise Security from the Row menu. Enter the password frequency specific to the user and save the entry.

3. Select the Reset Password Options checkbox and complete these fields, as necessary:
   - Password Expiry Notify Time

     Specify the time in hours and minutes the time of the day at which the user will be notified about the upcoming password expiration. This will be based on the local time of the user's country setup.
   - Password Expiry Notification Interval

     Specify the days before the password expiration on which the system should send notification to the user about the upcoming password expiration. You can define the days separated by commas, for example, to send notification three, five, and seven days before the password expiry date, enter 3,5,7 in this field.
   - Reset Password Link Active Time

     Specify the number of minutes for which the password reset link that the system sends on the user's email should be active. This field has a default value of 15.

     > **Note:** If you clear out the values in the above three fields, and deselect the Reset Password Options checkbox, the system disables the password reset self-service feature.
4. Click OK.

Reviewing User Sign-in Security History

If you know the specific user or role, you can review the user's or role's security history by using the EnterpriseOne Security application. You can also search for specific information for all users. For example, to see the users who were deleted on a given day, you can search on event type 06 **(Delete User)** and a specific event date.

Use the Security History form exit from the Work with User Security application (P98OWSEC) to review this history or audit records regularly according to your organization's security policy.

Prerequisite

The [SECURITY] section in the jde.ini on the security server must include the `History=1` setting for the system to record security history. This setting turns on the auditing for user sign-in and sign-off actions. Enabling this option will add the record in the F9312 and F9312T tables.

Forms Used to Review User Sign-in Security History

Form Name	FormID	Navigation	Usage
Work With User Security	W98OWSECE	Security Maintenance (GH9052), User Security (P98OWSEC)	Access forms to review security history.
Work With Security History	W98OWSECC	On the Work With User Security form, from the Form menu, select Security History.	Click Find to review the security history records.

Form Name	FormID	Navigation	Usage

Purge Audit Table Records

Security audit records can grow quickly and increase the size of the database. Therefore, you should set up a policy to purge security audit records regularly from the Security History table (F9312) using database tools. Keep a copy of these records for audit purposes.

Tracking User Activity (9.2 Update 6)

Starting with Tools Release 9.2.6, you can view the host name of the connecting client, the role of the user, pathcode, and environment used by the EnterpriseOne user during login, long user ID, server address, and the Application and Tools releases using the Work With Security History Long (P98LPSEC) application.

The P98LPSEC application uses the new F9312T table to track the user login information. This table also records the long user ID when long functionality is enabled in the Security History table.

You can use this information to block external access to the application by tracking the IP address or host name being used for accessing it. You can also use this information to track and audit the user activity details and to troubleshoot issues.

You can use these applications or reports to view the security tracking data:

- UX One Graphs (EnterpriseOne Pages)
- Application (P9312|W9312A)
- Orchestration Data Request
- Data Browser

Note: A UX One page records data from the P98LPSEC application and provides visibility into user access from various types of clients. See:

- *System Administrator Roles: System Administrator* in the *JD Edwards EnterpriseOne Applications UX One Roles User Guide* .
- *Enhanced User Security Activity Tracking Quick Tour*
- *Enhanced User Security Activity Tracking Tutorial*

Forms Used to Track User Activity

Form Name	Form ID	Navigation	Usage
Work With User Security	W98OWSECE	Security Maintenance (GH9052), and then User Security (P98OWSEC)	Access forms to review security history.
Work With Security History	W98OWSECC	On the Work With User Security form, from the Form menu, select Security History.	Click Find to review the security history records.
Work With Security History Long	W98LPSECK	On the Work With Security History form, from the Form menu, select Security History.	Click Find to review the security history detail records.
History Detail Form	W9312A	On the Work With Security History Long form, select the required user name, and select Detail from the Row menu.	Review the General, Reasons, and Connection Info tabs to view the login details.

Note: The above applications/forms can be secured using the application security. If the system is unable to determine the client information from where the login or logout events are triggered, UNKNOWN/Blank entries will be logged in the F9312T table and the P9312|W9312A form.

Tracking User Activity

1. Access the Work With User Security (P98LPSEC) application.
2. Click the **Form** menu, and select **Security History**.
3. In the Work With Security History Long form, click **Search**.
4. Select the required record, and then select **Detail** from the Row menu.

   The Security History Detail page is displayed.
5. In the **General** tab, review the information in the fields such as Event Status, Logoff Date, Logoff Time, Role, Pathcode, Environment, Apps Release, and Tools Release.
6. Click the **Reasons** tab and review the value in the Security Reason field.
7. Click the **Connection Info** tab and review the details in the Security Server and Client IP fields.

Managing Data Sources for User Sign-in Security

This section contains the following topics:

Understanding Data Source Management for User Sign-in Security

You add data sources to user and role records in user security to authorize users and roles to access EnterpriseOne databases. You can also revise the system user and password for existing data sources.

Forms Used to Manage Data Sources for User Sign-in Security

Form Name	FormID	Navigation	Usage
Work With User Security	W98OWSECE	Security Maintenance (GH9052), User Security (P98OWSEC)	Access forms to set up user security.
Add Data Source	W98OWSECS	On the Work With User Security form, from the Form menu, select Add Data Source.	Add a data source to a user, role, or all users.
Data Source Revisions	W98OWSECH	On the Work With User Security form, select a data source, and then select Revise Data Source from the Row menu.	Change the system user for a data source.
Remove Data Source	W98OWSECK	On the Work With Security form, select the appropriate record in the tree structure, and then click Delete.	Remove a data source. If you chose a data source for a specific user or role, this form displays the user ID or the role name with the data source name. If you chose only the data source, this form

Form Name	FormID	Navigation	Usage
			displays only the data source name.
Work With System Users	W980001A	In Solution Explorer, enter **P980001** in the Fast Path.	Locate a system user.
System User Revisions	W980001C	On the Work With System Users form, select a system user and then click the Select button.	Change the system user password.

Adding a Data Source to a User, a Role, or All Users

Access the Add Data Source form.

1. Complete one of these fields or options:
   - User ID

     Complete this field to add a data source to a specific user.
   - Role

     Complete this field to add a data source to a specific role.
   - All Users

     Select this option to add a data source to all users.
2. Complete these additional fields and click OK:
   - Data Source

     Leave this field blank to set the data source information for all data sources. When you leave this field blank, the system automatically enters **DEFAULT** in the field.
   - System User

Revising a Data Source for a User, Role, or All Users

Access the Work With User Security form.

1. Complete the Data Source field, and then click **Find**.

   > **Note:** You can also enter both a data source and user ID/role. If you select just a data source, the change will affect all users.

2. Select the data source in the tree structure and then, from the Row menu, select Revise Data Source.

   The Data Source Revisions form appears. If you chose a specific user or role, this form displays the user ID or the role name and the data source information. If you chose only the data source, this form automatically selects the All Users option with the data source information.
3. Complete the System User field and click **OK**.

   This field is necessary to access databases within the software. Depending on what you selected from the tree on the Work With User Security form, this information will apply to a specific user, a specific role, or all users.

Removing a Data Source for a User, Role, or All Users

Access the Work With User Security form.

1. Complete the Data Source field, and then click **Find**.
2. Select the appropriate record in the tree structure, and then click **Delete**.

   > **Note:** For a user, you can also select a row in the detail area for the user, and then click Delete.

   The Remove Data Source form appears. If you chose a data source for a specific user or role, this form displays the user ID or the role name with the data source name. If you chose only the data source, this form displays only the data source name.

   > **Note:** If you performed the search by data source without including a specific user or role, when you click OK on Remove Data Source, you remove the data source for *all* users.

3. Click **OK** to remove the data source.

Changing the System User Password

Access the Work With System User form.

1. Locate a system user and then click **Select**.
2. On the System Users Revision form, complete these fields and then click **OK**:
   - Password

     Enter a new password for the system user/data source combination.
   - Password Verify

     Enter the password again for verification purposes.

Enabling and Synchronizing the jde.ini Sign-in Security Settings

This section contains the following topics:

Understanding Security Setting Synchronization

You must modify the enterprise server and the workstation jde.ini files to enable and synchronize security settings between the enterprise server and the workstation.

> **Note:** For the EnterpriseOne workstations, enable security by changing settings in the workstation jde.ini file. You should make these changes on the deployment server-resident jde.ini file that is delivered to the workstation through a package installation.

Changing the Workstation jde.ini File for Sign-in Security

Access the jde.ini file.

1. Locate the jde.ini file that will be sent to the workstation as part of a package installation.

   This file is located on the deployment server in the release share path:

   ```
   \\xxx\CLIENT\MISC\jde.ini
   ```

   Where xxx is the installed release level of the software (for example, 810).
2. Using a text editor such as Notepad, view the jde.ini file to verify this setting:

   ```
   [SECURITY]
   SecurityServer=Enterprise Server
   ```

```
NameDefaultEnvironment=Default Environment
```

This table explains the variable values:

Setting	Value
Security Server	The name of the enterprise server. For workstations to sign on and run batch reports on the enterprise server, this value must be the same for both the workstation and the enterprise server.
DefaultEnvironment	A name that identifies any valid environment. If no value is specified, security is not enabled for that workstation.

Setting Auxiliary Security Servers in the Workstation jde.ini

Within the [SECURITY] section of the workstation jde.ini file, you can set as many as 10 auxiliary security servers. This example shows how the jde.ini file might look:

```
[SECURITY]
NumServers=Numeric Value
SecurityServer=Enterprise Server Name (primary)
SecurityServer1=Enterprise Server Name (auxiliary)
SecurityServer2=Enterprise Server Name (auxiliary)
```

This table explains the variable values:

Setting	Value
NumServers	The total number of security servers (primary and auxiliary) that you set under the [SECURITY] section of the jde.ini file. For example, if you set one primary and four auxiliary servers, the NumServers value is 5. You can set NumServers to any value between 1 and 10. If you do not include the NumServers setting, the system assumes that you have only one server.
SecurityServern	The name of an EnterpriseOne Enterprise Server. The primary and auxiliary security server names must all correspond to valid Enterprise Servers. The values for both the workstation and the Enterprise Servers must be the same for workstations to sign on to and run batch reports from the Enterprise Server. The variable value n can be a number between 1 and 10. This number defines the auxiliary security server.

Changing the Timeout Value Due to Security Server Communication Error

You might need to change a setting in the workstation jde.ini file if you receive an error such as:

```
Failure to Communicate with Security Server.
```

Change this section:

```
[JDENET]
connectTimeout=30
```

Changing the Enterprise Server jde.ini File for Security

Verify that the jde.ini file settings for security on the Enterprise Server are configured properly as described in this section. Use Server Manager to configure these settings which specify the internal security parameters, valid users and passwords, environments, and data sources.

In Server Manager, locate the configuration group settings for the Enterprise Server to verify these settings:

```
[JDENET_KERNEL_DEF4]
dispatchDLLName=name of host dll
dispatchDLLFunction=JDEK_DispatchSecurity
maxNumberOfProcesses=1
beginningMsgTypeRange=551
endingMsgTypeRange=580
newProcessThresholdRequests=0
[SECURITY]
Security Server=Enterprise Server Name
User=user ID
Password=user password
ServerPswdFile=TRUE/FALSE
DefaultEnvironment=default environment
```

This table explains the variable values:

Setting	Value
dispatchDLLName	Values for Enterprise Server host platforms are: • HP9000, libjdeknet.sl • RS/6000, libjdekrnl.so • Windows (Intel), jdekrnl.dll • Windows (Compaq AlphaServer), jdekrnl.dll • iSeries, JDEKRNL For UNIX platforms, values are case-sensitive.

Setting	Value
SecurityServer	The name of the Enterprise Server. This value must be the same for both the workstation and the Enterprise Server for workstations to run batch reports on the Enterprise Server.
User	The ID of a user with access to the F98OWSEC. This is the ID used to connect to the DBMS; therefore, this value must match that of the target DBMS.
Password	The password for the user ID with access to the F98OWSEC. This is the password used to connect to the DBMS; therefore, this value must match that of the target DBMS.
ServerPswdFile	This parameter is valid for servers operating under UNIX operating systems. The setting of this parameter determines whether the system uses special password handling for batch reports running on the server: • Set the value to TRUE to instruct the system to enable special handling of passwords. • Set the value to FALSE to disable special handling. When the system runs a batch report on the server, it runs the report using a string of line commands and parameters that includes the user password. Under UNIX operating systems, it is possible to use the process status command (ps command) to query the status of a job and view the parameters that were used to start the process. As a security measure, you can enable special handling by the software. When enabled, the software does not include the user password in the parameter list for a batch process. Instead, it includes the name of a file that contains the user password. This file is deleted as soon as the batch report reads the password.
DefaultEnvironment	The name of a valid environment for accessing the security table (for example, PD810).

Setting Auxiliary Security Servers in the Server jde.ini

Within the [SECURITY] section of the server jde.ini file, you can set one to 10 auxiliary security servers. Use Server Manager to configure these settings. You set multiple auxiliary security servers to establish levels of default servers. For example, if a machine cannot access a given security server, the machine tries the next security server that is defined in the [SECURITY] section. The settings for the auxiliary security servers might look like this example:

```
[SECURITY]
NumServers=Numeric Value
SecurityServer=Enterprise Server Name (primary)
SecurityServer1=Enterprise Server Name (auxiliary)
SecurityServer2=Enterprise Server Name (auxiliary)
```

This table explains the variable values:

Setting	Value
NumServers	The total number of security servers (primary and auxiliary) that you set under the [SECURITY] section of the jde.ini file. For example, if you set one primary and four auxiliary servers, the NumServers value

Setting	Value
	is 5. You can set NumServers to any value between 1 and 10. If you do not include the NumServers setting, the system assumes that you have only one server.
SecurityServerx	The name of an Enterprise Server. The primary and auxiliary security server names must all be valid enterprise servers. The values must be the same for both the workstation and Enterprise Servers for workstations to log onto and run batch reports from the enterprise server. The variable value x can be any number between 1 and 10. This number defines the auxiliary security server.

Verifying Security Processes in the Server jde.ini

You should define only one process for the security network. You can set multiple processes, but they are probably not necessary. In Server Manager, verify that the following parameter is set under the [JDENET_KERNEL_DEF4] section for the Server jde.ini file:

```
[JDENET_KERNEL_DEF4]
maxNumberOfProcesses=1
```

Managing Unified Logon

Note: Important: Unified Logon is deprecated with 9.2.2.0 tools release. You will not be able to use Unified Logon with any Tools Release greater than 9.2.2.0.

This section contains the following topics:

- *Understanding Unified Logon*
- *Modifying the jde.ini Setting to Enable or Disable Unified Logon*
- *Setting Up a Service for Unified Logon*
- *Removing a Service for Unified Logon*

Understanding Unified Logon

For configurations in which the Enterprise Server is on a Windows machine, to set up unified logon, you need to modify only the [SECURITY] section of the jde.ini file. When a user signs on, these settings alert the software to use unified logon.

When the Enterprise Server is on a non-Windows platform, you need to set up a Windows service for unified logon. This service identifies the unified logon server for EnterpriseOne. You also need to set the unified logon settings in the [SECURITY] section of the jde.ini file.

Note: When you use unified logon, you need to use the same user ID for the Windows domain and JD Edwards EnterpriseOne so that the records for each are synchronized. For example, if the user ID for a user in the Windows domain is USER1, the user ID for EnterpriseOne must also be USER1. If the user IDs are different, unified logon does not work for the user.

Modifying the jde.ini Setting to Enable or Disable Unified Logon

Locate the Security configuration settings for the Enterprise Server and the jde.ini file settings on the workstation.

To modify the settings to enable or disable unified logon:

1. In Server Manager, modify the Security Mode setting in the Security settings for the Enterprise Server. Valid values are:
   - **Standard Sign-on Only**. Accepts only users set up for standard sign-in security.
   - **Unified Logon Only**. Accepts only users set up for unified logon.
   - **Standard and Unified Logon**. Accepts users set up for both unified logon and standard sign-in security.
2. In the workstation jde.ini file, add these settings in the [SECURITY] section:

```
[SECURITY]
UnifiedLogon=0 or 1
```

Value	Description
0	Disables unified logon for the workstation. This setting is the default value.
1	Sets unified logon for the workstation.
server_name	Enter the name of the server on which the unified logon server data resides.

Setting Up a Service for Unified Logon

If the Enterprise Server is not a Windows server, you should set up services for unified logon on the Deployment Server. The Deployment Server is always a Windows server.

To set up a service for unified logon:

1. On the deployment server, in Windows Explorer, access the \Unified Logon directory and run the file UniLogonSetup.exe.

   The Unified Logon Server Setup form appears. On this form, you define the Windows service for unified logon servers. You can also remove these services on this form.

2. Complete these fields:
   - Unified Logon Service Name

     Enter the name for the unified logon server.
   - EnterpriseOne Port Number

     The port number for the unified logon server should match the EnterpriseOne port number of the server for which you want to set up unified logon.
   - Service Executable Filename

     Enter the directory path for the unified logon service program.
   - Log Filename

     Enter the name of the unified logon log file, including the full directory path.

     The default user list contains all authenticated network users.
3. To create a custom user list, enter the users or the groups in the Users or User Groups box to add the user information to the unified logon user list.

   Note: Generally, the default Windows list of authenticated network users lists users by group.
4. Click the **Install Service** button to save the service information for the unified logon server.

Removing a Service for Unified Logon

To remove a service for unified logon:

1. Run UniLogonSetup.exe.

   The Unified Logon Server Setup form appears.
2. From the Unified Logon Service Name menu, select a unified logon server, and then click the **Uninstall Service** button.

13 Enabling Long Passwords in EnterpriseOne

Enabling Long Passwords in EnterpriseOne

In EnterpriseOne Tools 9.2, in addition to the feature for enabling long passwords, Oracle provides an option to enable the creation of long user IDs up to 254 characters in length. The Long Password and Long User features are autonomous, that is, you can enable one without enabling the other. For more information about enabling long user ID support in EnterpriseOne, see *Setting Up Long User IDs in EnterpriseOne*.

Understanding the Long Password Feature

As with releases prior to EnterpriseOne Tools 9.2, out of the box, EnterpriseOne passwords are limited to a maximum of 10 characters (referred to as "short" passwords in this chapter). With EnterpriseOne Tools 9.2, administrators have the OPTION to enable the Long Password feature, which enables users to create case sensitive passwords up to a maximum of 40 characters.

To create and revise short passwords, you use P98OWSEC. To enable the Long Password feature and create long passwords, you use P98LPSEC. When the Long Password feature is enabled, P98OWSEC is no longer accessible in EnterpriseOne; users and administrators must access P98LPSEC to change their long passwords.

Understanding Password Policy Rules When the Long Password Feature is Enabled

If the Long Password feature is **not** enabled, password policy rules for short passwords are defined in the P98OWSEC processing options. For User Profile Self-Service application (P0092SS) users, the password policy rules are defined in the Global Password Policy form.

As part of enabling the Long Password feature, EnterpriseOne detects if there are existing password policy rules defined in the P98OWSEC processing options and migrates these rules into the Global Password Policy form. The system then uses the rules defined in the Global Password Policy form for all EnterpriseOne users, including P0092SS users. This establishes a single set of password policy rules for passwords for easier maintenance.

You can define the following rules for long passwords in the Global Password Policy form:

- Minimum Password Length
- Minimum Number of Numerics
- Maximum Consecutive Characters
- Minimum Number of Characters
- Minimum Number of Special Characters

CAUTION: Remember that long passwords are case sensitive. EnterpriseOne checks the case of password characters when the Long Password feature is enabled.

EnterpriseOne Systems and Integrations that Support Long Passwords

When the Long Password feature is enabled, most EnterpriseOne systems that require EnterpriseOne credentials for access or for processing will accept long passwords. This includes but is not limited to the following features and functionality:

- EnterpriseOne web client and EnterpriseOne Windows client.
- Server Manager Console.

  The Server Manager Console supports long passwords, but it does not support long user IDs. If the Long User feature is enabled, Server Manager users must continue to use a short user ID.
- Transactions and reports that require credentials for processing.
- EnterpriseOne auditing features including the auditing of security records and 21 CFR auditing.
- Single sign-on configurations, including single sign-on with Oracle Access Manager (OAM).
- EnterpriseOne configurations with LDAP systems for managing users. An LDAP configuration does require specific settings for supporting long passwords. See *Enabling LDAP Support in JD Edwards EnterpriseOne* for details.
- Other EnterpriseOne systems or components that requires user credentials for access or processing, such as the Scheduler application, the Configuration Assistant and Change Assistant, RUNUBE and RUNUBEXML, the wizard for developing business services, EnterpriseOne mobile clients and supported tablet clients, and so forth.

Considerations for an EnterpriseOne Multiple Foundation Configuration

If you plan to enable both the Long User feature and Long Password feature in a multiple foundation configuration, you must perform additional configuration steps before enabling the Long Password feature.

Prerequisites for a Multiple Foundation Setup

Before you enable the Long Password feature, you must perform the steps in this section depending on your configuration scenario:

Scenario 1

If you have enabled the Long Password feature and if you have more than one EnterpriseOne Enterprise Server sharing the same F98OWSEC table, you must update all Enterprise Servers to EnterpriseOne Tools 9.2 to support both long user IDs and long passwords.

Scenario 2

If you want to enable the Long Password feature and you do not update all EnterpriseOne Enterprise Servers to EnterpriseOne Tools 9.2, then you need to create two Security Server data sources: one for Enterprise Servers on Tools 9.2 and one for Enterprise Servers on a release prior to EnterpriseOne Tools 9.2. In this multiple foundation setup, only the Enterprise Servers on EnterpriseOne Tools 9.2 will support long user IDs and long passwords. For this type of configuration, you must perform the following steps before enabling the Long Password feature:

1. Create an additional (new) system data source, for example:

   SYSTEM - 900MF or SYSTEM - 910MF or SYSTEM - 920MF
2. Copy the following security tables to this new data source:

   F0092, F00921, F00927, F0093, F00941, F9312, F98OWPU, F98OWSEC, F0092L
3. Change the SYSTEM and Server Map in all environments with EnterpriseOne Tools 9.2 and above so that the following tables are pointed to the newly created data source (SYSTEM - 900MF or SYSTEM - 910MF or SYSTEM - 920MF):

   F98OWSEC, F00921, F98OWPU, F0092, F00927

   > **CAUTION:** Do not create any OCM mappings (client or server) that point to the newly created data source. Only change the records for the preceding tables to point to new data source in existing SYSTEM and Server Maps.
4. On the Security Server on EnterpriseOne Tools 9.2 or above, change the Boot Strap Data Source to point to the newly created data source. To do so, use Server Manager to locate and update the following setting, which is a setting in the jde.ini file on the Security Server.

   ```
   [SECURITY]
   DataSource=<new data source name>
   ```

Enabling the Long Password Feature

Enabling the Long Password feature allows users to create passwords up to a maximum of 40 characters. After the Long Password feature is enabled:

- P98OWSEC is disabled and EnterpriseOne directs you to P98LPSEC to create and manage user sign-in security records.

  P98LPSEC contains the same features and functionality as P98OWSEC. Therefore, when working with user sign-in security in P98LPSEC, you can refer to the steps in *Setting Up User Sign-in Security* in this guide.
- Users can continue to use their existing "short" passwords for sign-in, as long as their passwords meet the criteria defined in the password policies.
- After this feature is enabled, an administrator must use the Global Password Policy form to modify password policies.

To enable the long password feature:

1. Access P98LPSEC.

2. On Enable Long Password, select the **Enable Long Password** check box.
3. Click **Submit**.
4. On the Confirmation dialog box, click **Yes** if you want to continue and enable the Long Password feature.

   The Confirmation box informs you that the feature cannot be disabled after it is enabled.

   It also displays a notice if it detects that password rules have been set up for P0092SS, and informs you that these password rules will be overridden with password rules defined in the processing options in P98OWSEC.

   EnterpriseOne displays the Global Password Policy form with the values automatically migrated from the password policy processing options in P98OWSEC.
5. On Global Password Policy, define the password rules for long passwords by completing the following fields:

   - **Minimum Password Length**. The minimum password length that the system allows when a user changes his or her password.
   - **Minimum Number of Numerics**. The minimum number of numeric characters that each password must contain. For example, if you enter 3 in this field, the system allows the passwords h584htnuud and h584htn6ud, but does not allow the password h5h4htnuud.
   - **Maximum Consecutive Characters**. A value that indicates the maximum number of identical, consecutive characters that the system allows users to include in their passwords. For example, if you set this value to 2, the system allows Tops or Tools but not Bosss.
   - **Minimum Number of Characters**. The minimum number of characters that the system allows in a password.
   - **Minimum Number of Special Characters**. The minimum number of special characters that the system allows in a password. If you leave this blank, users have the option to include special characters, but are not required to do so.

     > **CAUTION:** If you update a password rule that prevents users from using an existing password, then you must use the "Force Immediate Password Change" option to force users to change their passwords during the next sign on. See *Revising All User Sign-in Security*.
6. Click **OK** to save the password policy rules.
7. Access Server Manager and restart the EnterpriseOne Enterprise Server and the EnterpriseOne HTML Server for the changes to take effect.

To verify that the Long Password feature has been enabled:

1. On an EnterpriseOne Windows client, access the Universal Table Browser.
2. On Table and Data Source Selection, select **Open Table** from the File menu.
3. On Table and Data Source Selection, complete these fields:

   - **Table**. Enter `F98OWSEC`.
   - **Data Source**. Enter the data source in which you enabled the Long Password feature.
4. In the F98OWSEC table, verify that the first record contains a value of *LPENABLE, which indicates that the Long Password feature is enabled.

   Also, if the second row contains a *POLICY record, this indicates that global password policies have been migrated from the processing options in P98OWSEC.

Changing Long Passwords

After the Long Password feature is enabled, administrators and users are directed to P98LPSEC application instead of P98OWSEC to update long passwords. Users and administrators can update long passwords according to the rules defined in the Global Password Policy form.

To update a long password:

1. On Work With User Security (P98LPSEC), to change the password of a user, enter the user ID of the user in the User ID/Role field and click the **Find** button.

   You can also enter a long user ID if the system has been enabled for long user IDs.
2. On the tree in the left area, select the user ID.
3. From the Form menu, select **Admin Passwords Rev**.
4. On Administration Password Revisions, complete the following items:
   - **User ID**. This field contains the user ID selected on the Work With User Security form.
   - **New Password**. Enter a new password.
   - **New Password - Verify**. Enter the password again to verify it.
   - **Force Immediate Password Change**. Click this check box to force the user to change the password during the next sign-in.
   - **Change Password in Scheduler Table**. This check box is selected by default. This ensures that the new password is accepted by the Scheduler application.
5. Click **OK**.

Modifying Password Rules for Long Passwords

When the Long Password feature is enabled, use the Global Password Policy form to create password rules for all users in EnterpriseOne including User Profile Self-Service application (P0092SS) users.

> **Note:** If the Long Password feature is not enabled, than the rules defined in this application apply only to User Profile Self-Service application users.

To modify or customize password rules:

1. Access P98OWSEC.
2. On With User Security, select the **Form** menu, **GlobalPasswordPolic**.
3. On Global Password Policy, complete the following fields to set up password rules:
   - **Minimum Password Length**
   - **Minimum Number of Numerics**
   - **Maximum Consecutive Characters**
   - **Minimum Number of Characters**
   - **Minimum Number of Special Characters**

4. Click **OK**.

14 Enabling LDAP Support in JD Edwards EnterpriseOne

Enabling LDAP Support in JD Edwards EnterpriseOne

Note: This chapter does not provide instructions for installing and configuring an LDAP-compliant directory service, such as Microsoft Windows Active Directory or IBM Directory Server. For more information, refer to the *Prerequisites* section in this chapter.

Understanding LDAP Support in JD Edwards EnterpriseOne

This section contains the following topics:

- *LDAP Support Overview*
- *User Profile Management in LDAP-Enabled JD Edwards EnterpriseOne*
- *LDAP and JD Edwards EnterpriseOne Relationships*
- *Application Changes in LDAP-Enabled JD Edwards EnterpriseOne*
- *LDAP Server-Side Administration*
- *JD Edwards EnterpriseOne Server-Side Administration*

LDAP Support Overview

LDAP is an open industry standard protocol that directory services use to manage user profiles, such as user IDs and passwords, across multiple application systems. You can enable EnterpriseOne to use an LDAP-compliant directory service to manage EnterpriseOne user profiles and user-role relationships. After enabling EnterpriseOne for LDAP, user profiles can be administered through an LDAP version 3 compliant directory server, otherwise referred to as the LDAP server. System administrators use a third-party LDAP-enabled application to access the LDAP server.

LDAP provides these benefits:

- Central administration and repository for user profiles.

  You can easily maintain user profiles in a single location that serves multiple end user applications, including EnterpriseOne applications.
- Reduced complexity.

  You are not required to use several applications to maintain user profiles. In addition, users are not required to maintain multiple passwords across multiple systems.

Note: LDAP support does not address single sign-on functionality that might exist through other EnterpriseOne functionality.

User Profile Management in LDAP-Enabled JD Edwards EnterpriseOne

When EnterpriseOne is enabled for LDAP, the features used to Add, Copy or Delete user profiles in the Work with User/Role Profiles application (P0092/W0092D) are disabled. Instead, you must use a third-party, LDAP-enabled application to manage EnterpriseOne user profiles.

You can manage existing user profiles in User Profile Revisions (P0092/W0092A).

Note: EnterpriseOne does not provide an application for managing LDAP user profiles.

Additionally, EnterpriseOne provides a self-service version of P0092. This self-service application is used to manage only self-service user profile information for the Manufacturing Sourcing module; not EnterpriseOne user profiles. However, if you are enabling EnterpriseOne for LDAP and your company is using this self-service application, you can add parameters for it when you define the LDAP server settings. In this configuration, any self-service user profiles that are added are synchronized with the LDAP server.

Note: Even though self-service user profiles are synchronized with the LDAP server, you cannot use this self-service application to manage EnterpriseOne or LDAP user profiles.

See *Configuring the LDAP Server Settings*.

LDAP and JD Edwards EnterpriseOne Relationships

The LDAP system administrator must understand the logical and database-dependent relationships between the LDAP server and EnterpriseOne. The administrator directly or indirectly controls the logical flow of events and where specific data resides based on the setting of system variables in the EnterpriseOne Enterprise Server jde.ini file and settings specified in the LDAP Server Configuration Workbench application (P95928).

The security kernel on the Enterprise Server is responsible for ensuring the integrity of the security within EnterpriseOne. If this kernel is not running correctly or cannot locate requisite data, users cannot sign in to EnterpriseOne. However, when the security kernel is properly configured, the system verifies the user credentials from data within the user profiles. In this case, the following two scenarios are possible:

- You can configure EnterpriseOne to use LDAP to manage user profiles.
- You can configure EnterpriseOne to use LDAP to manage user-role relationship data.

LDAP does not support certain user profile information. Such information remains in the domain of the EnterpriseOne Server and must be maintained by the EnterpriseOne system administrator. Therefore, two distinct and separate user profiles may exist:

- LDAP user profile

  This profile includes the user ID and password and can include user-role relationships.

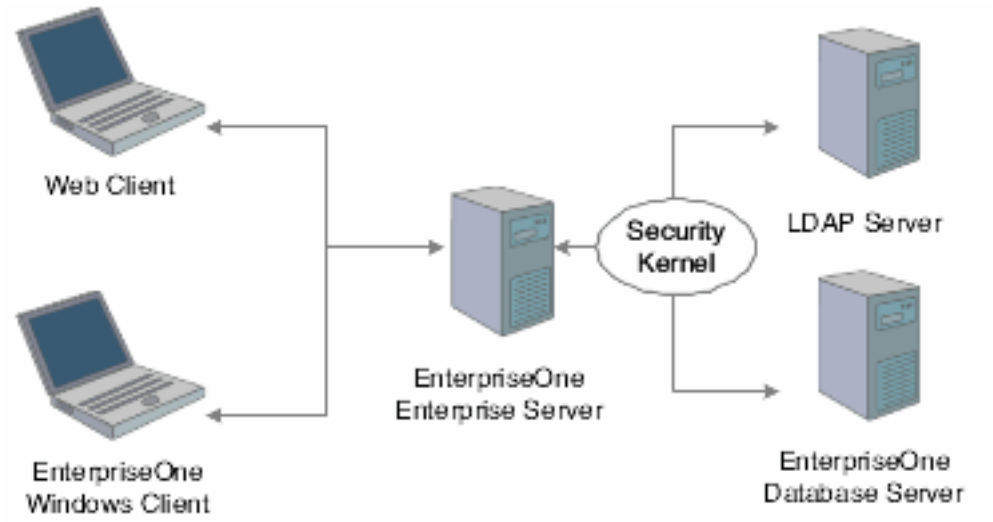
- JD Edwards EnterpriseOne user profile

  The information contained in this profile is stored in the EnterpriseOne database. Examples of such information include the date separator, the decimal separator, and so on.

User Authentication Using the LDAP Server

When LDAP is enabled, all systems (including EnterpriseOne) are directed to perform user authentication through the LDAP server.

This diagram shows how LDAP and EnterpriseOne handle authentication:



In this illustration, the security kernel in the Enterprise Server performs authentication against the LDAP server when LDAP is enabled in the [SECURITY] section of the jde.ini file of the Enterprise Server. Otherwise, when LDAP is disabled, the security kernel authenticates the user against the Enterprise Server database.

JD Edwards EnterpriseOne User Data

The security kernel in EnterpriseOne requires specific attributes to be defined for all users. These attributes generally include:

- User ID.
- User password.
- User-role relationship.
- JD Edwards EnterpriseOne system user.
- Definition of role.
- JD Edwards EnterpriseOne user profile settings.

User Data Managed by LDAP

When you configure EnterpriseOne to use LDAP, the EnterpriseOne security kernel uses the following data stored in the LDAP server:

- User ID
- User password
- User-role relationship (optional)

Data Managed by LDAP and JD Edwards EnterpriseOne

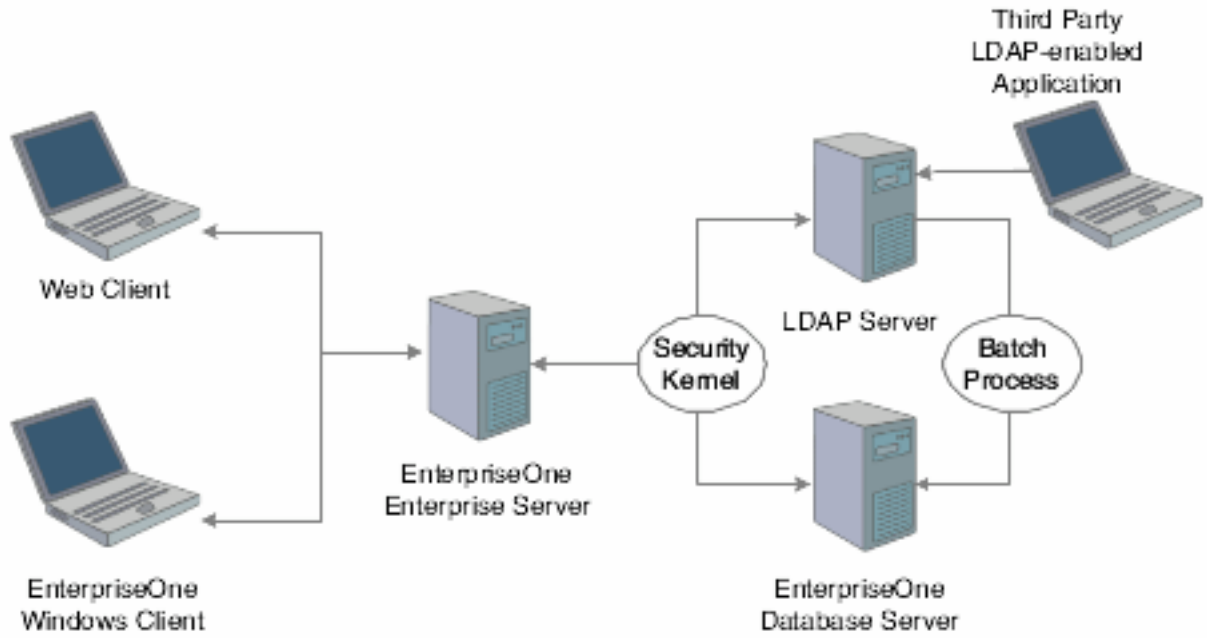
This table explains how user data is managed by LDAP and EnterpriseOne, as well as how the security kernel uses this information:

Data Category	LDAP	EnterpriseOne	Comment
EnterpriseOne User ID	Yes	Yes F0092	If you enable LDAP support in EnterpriseOne, the security kernel validates the user from the LDAP database. The security kernel synchronizes this data from LDAP to EnterpriseOne only when this data is in the LDAP server and not in EnterpriseOne.
Enterpriseone Long User ID	Yes	Yes F0092L	Long user ID to short user ID mapping table.
EnterpriseOne User Password	Yes	Yes F98OWSEC	If LDAP is enabled, the user password is always stored in LDAP. If LDAP is not enabled, the user password is stored in the F98OWSEC table in EnterpriseOne.
User-Role Relationship	Yes	Yes F95921	If the user-role relationship is defined to execute through LDAP, the user-role relationship is synchronized from the LDAP server to EnterpriseOne. If the user-role relationship is defined to execute through EnterpriseOne, the data is stored in the EnterpriseOne database in the F95921 table.
EnterpriseOne System User	No	Yes F98OWSEC	Not managed in the LDAP server. EnterpriseOne requires each user to have a system user specified for access to the EnterpriseOne database. The database user is set by the EnterpriseOne system administrator in the EnterpriseOne security table, F98OWSEC. If there are no valid system user settings, the EnterpriseOne security kernel will not validate the user.
Definition of Role	Yes	Yes F0092	The user-role relationship is synchronized from the LDAP server to the EnterpriseOne database for roles defined in the EnterpriseOne database. However, the system does not synchronize role definitions from the LDAP server to the EnterpriseOne database. Therefore, role definitions must exist in both systems.
EnterpriseOne User Profile Attributes	No	Yes F00921 and F0092	Not managed in LDAP. EnterpriseOne requires additional user profile attributes that are not generally defined through

Data Category	LDAP	EnterpriseOne	Comment
			equivalent attributes in LDAP. Therefore, you can manually set these attributes. You can also specify these values in the default user profile settings for LDAP so that these settings are included for each user that is synchronized from LDAP to EnterpriseOne. See *Modifying the LDAP Default User Profile Settings*. Some of these attributes include: • Address Book Number • Decimal Separator • Time Zone • Currency • Date Format

User Data Synchronization in LDAP-Enabled JD Edwards EnterpriseOne

This diagram shows the synchronization of user data from the LDAP server to EnterpriseOne:



In this configuration, a third-party LDAP-enabled application is being used to add, modify, and delete LDAP user information. In addition, the system uses the following methods to synchronize user data from LDAP to the EnterpriseOne database:

- At user sign-in, using the EnterpriseOne security kernel.
- Using the LDAP Bulk Synchronization batch application (R9200040).

  R9200040 enables you to perform bulk synchronization of user profile records from the LDAP server to the EnterpriseOne database.

Application Changes in LDAP-Enabled JD Edwards EnterpriseOne

When LDAP support is enabled in EnterpriseOne, some of the user profile tasks that you typically perform in EnterpriseOne, such as adding and deleting users, are disabled. You must use LDAP to modify these records, not EnterpriseOne. This section summarizes the following changes in EnterpriseOne menus and applications that result from using LDAP to manage user profile information:

- User password changes.
- User Profile Revisions application changes.
- Security Revisions application changes.
- Role Relationships application changes.
- Scheduler application changes.

User Password Changes

In EnterpriseOne, users can change their passwords using the User Default Revisions application. However, when LDAP is enabled, users must contact a system administrator for password changes. If a user attempts to select the Change Password option in the User Default Revisions form, the system displays this error:

```
Error: LDAP authentication is enabled.
Solution: Users must contact a security administrator to have their passwords#
 changed.
```

User Profile Revisions Application (P0092) Changes

The following functions for managing user information in P0092 are disabled:

- Add
- Copy
- Delete

This ensures that users can only be managed through LDAP.

EnterpriseOne Security Application (P98OWSEC) Changes

When LDAP is enabled, P98OWSEC only allows you to add or change specific security settings for specified users. This section discusses the features that you can use in this application when LDAP is enabled.

When an existing *single* user is selected for security revisions, the User ID field contains the selected user ID.

On the Security Detail Revisions form, you can enable the User Status and Allowed Password Attempts fields by selecting these corresponding options:

- User Status
- Attempts

When you are updating security for *all* users, you click the Revise All button from the Form menu in the Work With User/Role Profiles form. The Security Detail Revisions form appears.

On the Security Detail Revisions form, you can enable the User Status and Allowed Password Attempts fields for all users by selecting these corresponding options:

- User Status

- Attempts

Role Relationships Application (P95921) Changes

When LDAP is enabled, P95921 has been modified to enable or disable certain functionality, depending on whether roles are managed in LDAP. When roles are managed in LDAP, you cannot use EnterpriseOne to add or delete a role for an individual user. However, you can add roles to the default user for LDAP, which is _LDAPDEFLT. Additionally, you can modify the role expiration date.

If you attempt to add a role to an individual user in EnterpriseOne, the system displays this error:

```
Error: Role Relationship is managed by LDAP.
```

Similarly, if you attempt to delegate, remove, or add a role for an individual user, the system will display the same error.

> **Note:** When LDAP is enabled and roles are managed in LDAP, you can use a third-party LDAP-enabled application to add, delete, or modify role relationships for any user.

Schedule Jobs Application Changes

The Schedule Jobs application (P91300) displays a password column which is written to the F91300 table. The password stored in this column provides the password that P91300 uses to connect to the EnterpriseOne database. The column is only stored for program use and the actual database record contains an encrypted blob that cannot be viewed or decrypted by the system administrator. However, you can enter the password in the Scheduler Password field of the Scheduling Advance Options form.

The Scheduler kernel validates the user ID and password stored in F91300. The job cannot be launched if the validation fails. Therefore, if the user changes their password after the job is scheduled, the job cannot be launched. In such cases, the user must use P91300 to revise the job.

LDAP Server-Side Administration

This section assumes that EnterpriseOne is using the LDAP server for user profile administration. Using a third-party LDAP-enabled application to access the LDAP server, you can add, modify, or delete attributes of user profiles. This table lists the items that you can manage and actions that you can perform from the LDAP server:

User Profile Attribute	Action	Description
User ID and Password Values	Add Modify Delete	The user ID and password values must be alphanumeric and cannot exceed 10 characters in length. Unicode is supported. If the Long User ID feature is enabled in EnterpriseOne, you can enter a user ID up to 254 characters in length. If the Long Password feature is enabled in EnterpriseOne, you can enter a password up to 40 characters in length. At sign-in, logic on the EnterpriseOne server automatically performs one-way, real-time synchronization of user IDs from the LDAP server to the EnterpriseOne database.

User Profile Attribute	Action	Description
		You can run a separate batch application on the Enterprise Server to initially migrate user IDs from LDAP to the EnterpriseOne database.
User-Role Relationship	Add Modify Delete	At sign-in, logic on the EnterpriseOne server will automatically perform one-way real-time synchronization of this data from the LDAP server to the EnterpriseOne database. You can run a separate batch application on the EnterpriseOne server to initially migrate this data from LDAP to the EnterpriseOne database. Only valid EnterpriseOne user-role relationships will be synchronized from LDAP to the EnterpriseOne database.
Role Definitions	Add Modify Delete	You must manually set up role definitions in LDAP and EnterpriseOne because there is no automated method to synchronize this data.

JD Edwards EnterpriseOne Server-Side Administration

When EnterpriseOne is enabled for LDAP, there are still some user profile administrative tasks that you manage on the Enterprise Server, such as:

- Tasks that are not supported by LDAP.
- Tasks that are not synchronized automatically.
- Tasks that are not synchronized through a batch process.

You can modify the following items on the Enterprise Server:

EnterpriseOne Attributes	Action	Description
System User ID and Password	Add Modify Delete	Required to set system values not supported by LDAP. System information is used to connect to the database. It includes database system user name, system user password, and data source name (system key).
User-Role Relationship	Add Modify Delete	Required if user-role relationships are managed in EnterpriseOne.
User-Role Relationship Attributes	Add Modify	Required to set attributes not supported by LDAP, such as *ALL and Expiration Dates, when you manage user-role relationships in LDAP.

EnterpriseOne Attributes	Action	Description
	Delete	
User Status	Modify	Allowed statuses include: • Enabled • Disabled There is no automatic or batch synchronization between LDAP and EnterpriseOne for this function.
Allow Password Attempts for EnterpriseOne User	Modify	The number of invalid sign-on attempts a user can make before that user profile is disabled.
Role Definitions	Modify	You must always define the role definition in EnterpriseOne, regardless of any LDAP considerations.

Configuring LDAP Support in JD Edwards EnterpriseOne

This section contains the following topics:

Note: If you are creating an LDAP configuration for Oracle Internet Directory, the specific settings for this configuration are listed in an appendix in this guide. See *Creating a JD Edwards EnterpriseOne LDAP Configuration for OID*.

Overview of Steps to Enable LDAP Support in JD Edwards EnterpriseOne

You must follow these high-level steps in the specified order to properly configure the Enterprise Server to support LDAP:

1. Disable LDAP authentication on the Enterprise Server. In Server Manager, in the Enterprise Server configuration settings, make sure that the **Enable LDAP Authentication** check box in the Security settings is cleared.
2. Use the LDAP Server Configuration Workbench application (P95928) to create an LDAP configuration, configure the LDAP server settings, and configure the LDAP to Enterprise Server mappings. The P95928 application is available on the Microsoft Windows client and the web client.

   > **Note:** EnterpriseOne provides two versions of this application. You can use ZJDE0001 to create a template for creating an LDAP configuration. Create the template by adding specific attributes to the LDAP configuration that can be defined later. This section uses ZJDE0002 of the application to show all possible attributes that can be mapped in the LDAP configuration.

3. Use the Configure LDAP Defaults form to enter the required LDAP default user profile settings.

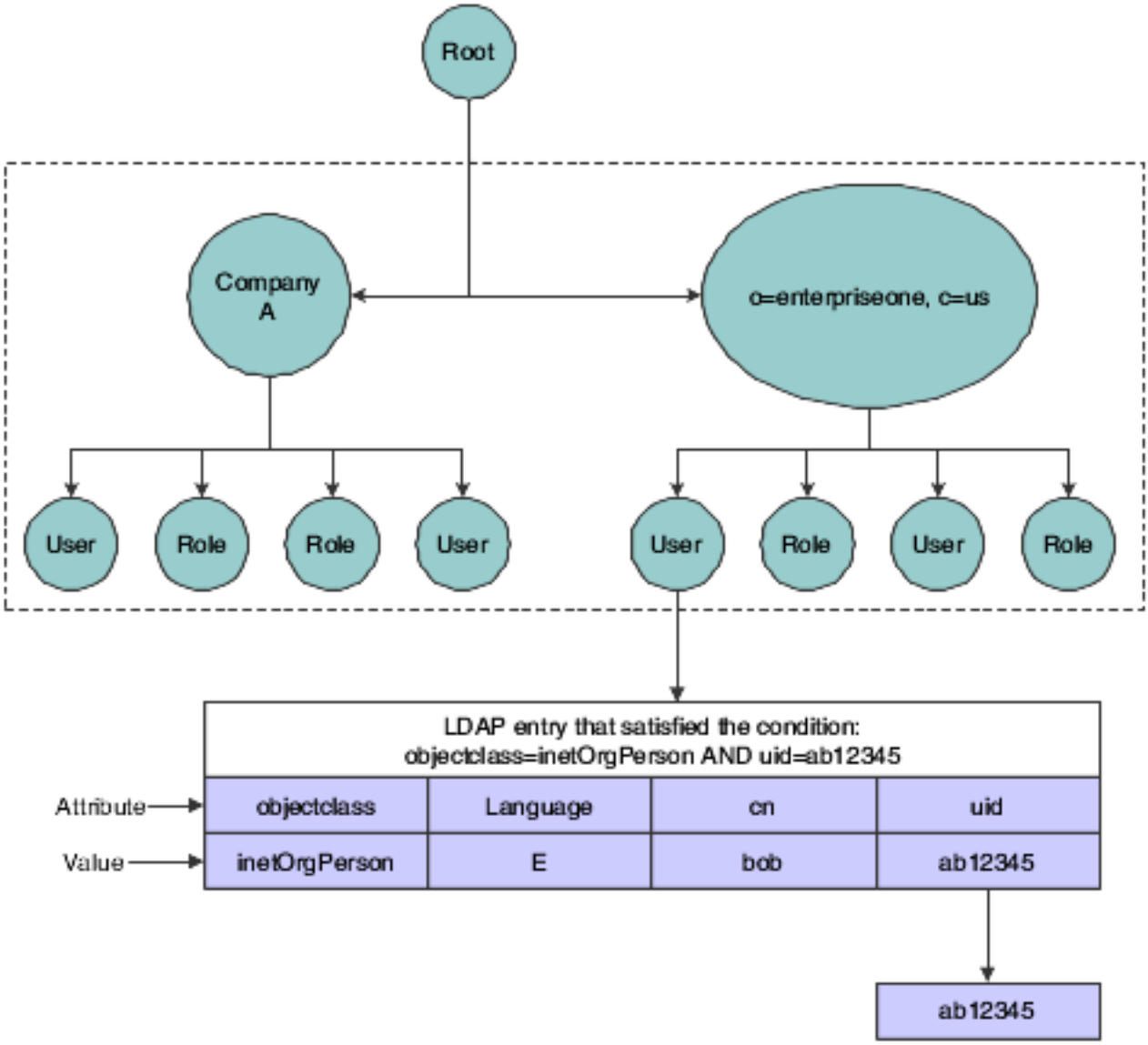
   See *Modifying the LDAP Default User Profile Settings*.
4. Change the LDAP configuration status.
5. Enable LDAP authentication on the Enterprise Server. In Server Manager, click the **Enable LDAP Authentication** check box in the Enterprise Server Security configuration settings.
6. Restart the Enterprise Server.

How JD Edwards EnterpriseOne Uses LDAP Server Settings

Part of creating an LDAP configuration for EnterpriseOne involves configuring LDAP server settings. The LDAP server settings are in compliance with the standard syntax specified by the LDAP Data Interchange Format (LDIF). These settings, or attributes, when configured correctly, determine how EnterpriseOne searches for user profile data in the LDAP server. The attributes that you configure differ depending on whether you are:

- Creating a standard EnterpriseOne configuration for the LDAP server.
- Using Secure Socket Layer with the LDAP server.
- Using the self-service version of the user profile application for the Manufacturing Sourcing module.
- Using EnterpriseOne long user IDs.

This diagram shows how EnterpriseOne uses the LDAP server settings to search for user profiles in the LDAP server:



In this diagram, the EnterpriseOne application requests a search of the Directory Information Tree for a EnterpriseOne user in the United States with an ab12345 user ID. The user can only be found if these attributes contain valid values:

Attribute	Value
USRSRCHBAS (User Search Base)	o=enterpriseone, c=us
USRSRCHSCP (User Search Scope)	subtree
USRSRCHFLT (User Search Filter)	objectclass=inetOrgperson
USRSRCHATR (User Search Attribute)	uid

Attribute	Value
E1USRIDATR (EnterpriseOne User ID Attribute)	uid

1. EnterpriseOne starts the search using the criteria specified in the User Search Base attribute.
2. EnterpriseOne uses the value in the User Search Scope attribute to determine the scope of the search.
3. EnterpriseOne uses the following Search Filter parameter to search for the user in LDAP:

```
(&((User Search Filter value), ((User Search Attribute value)= "ab12345")))
```

4. EnterpriseOne retrieves the user ID from the EnterpriseOne User ID Attribute.

Understanding an LDAP Configuration with EnterpriseOne Long User IDs

In an EnterpriseOne long user ID configuration, the USRSRCHATR should point to an LDAP attribute holding the long user ID. This LDAP attribute should be capable of holding up to 254 characters.

Some LDAP servers such as Microsoft Active Directory limit the distinguished name (also known as DN) of the user to 255 total characters. If you attempt a simple LDAP bind with more than 255 characters, you might experience authentication errors. Therefore, it is your responsibility to make sure long user IDs on these LDAP servers adheres to these limits. For more information about setting up long user IDs in EnterpriseOne, see *Setting Up Long User IDs in EnterpriseOne*.

This table, *LDAP Configuration Settings for Long User IDs* shows an example of LDAP configuration settings for long User IDs. Notice that the USRSRCHATR is pointing to LDAP attribute 'cn' while E1USRIDATR is pointing to LDAP attribute 'uid'. This is different from a non-long user ID configuration where both E1USRIDATR and USRSRCHATR point to same LDAP attribute.

LDAP Configuration Settings for Long User IDs

Attribute	Value
USRSRCHBAS (User Search Base)	o=enterpriseone, c=us
USRSRCHSCP (User Search Scope)	subtree
USRSRCHFLT (User Search Filter)	objectclass=inetOrgperson
USRSRCHATR (User Search Attribute)	cn
E1USRIDATR (EnterpriseOne User ID Attribute)	uid

Prerequisites

To configure LDAP support in EnterpriseOne, you must have a system administrator who understands LDAP and understands how to use an LDAP-compliant directory service to manage user profile information.

For more information on LDAP, refer to these resources on the web:

- The IETF LDAPv3 Working Group.

  See `https://datatracker.ietf.org/wg/ldapbis/charter/`
- The LDAPv3 Working Group archived newsgroup.

  See `http://www.openldap.org/lists/ietf-ldapbis/`
- RFC 3377, the current definition of LDAPv3.

  See `http://ftp.rfc-editor.org/in-notes/rfc3377.txt`

For more information about a specific LDAP-compliant directory service, refer to that particular directory service's documentation.

If you are configuring the directory service with SSL/TLS (Transport Layer Security), refer to the directory service documentation for instructions.

Forms Used to Configure LDAP Support in JD Edwards EnterpriseOne

Form Name	FormID	Navigation	Usage
Available LDAP Configurations	W95928F	Enter **P983051** in the Fast Path. On the Work With Interactive Versions form, enter P95928 in the Interactive Version field and click Find. Select ZJDE0002 and then select Run from the Row menu. The P95928 application is available on the Microsoft Windows client and the web client.	Add an LDAP configuration record.
LDAP Server Information	W95928A	On the Available LDAP Configurations form, click Add.	Complete the fields that are required for the LDAP configuration record.
LDAP Server Attribute Values	W95928E	On the Available LDAP Configurations form, select a configuration record and then select Values from the Row menu.	Enter LDAP server attribute values.
LDAP Server Mappings	W95928B	On the Available LDAP Configurations form,	Configure LDAP to EnterpriseOne

Form Name	FormID	Navigation	Usage
		select Mappings from the Row menu.	Enterprise Server mappings.

Creating an LDAP Configuration

Access the Available LDAP Configurations form.

1. Click **Add** to add a new configuration record.
2. On the LDAP Server Information form, complete these fields and then click **OK**:

Field	Description
Server Configuration Name	Enter a unique name for the server configuration, and then tab to the next field and enter a description.
Enterprise Server Location	Enter the location of the Enterprise Server.
Enterprise Server Port	Enter the port used to connect to the Enterprise Server.
LDAP Server Location	Enter the location (machine name or IP address) of the LDAP server on the network.
LDAP Server Port	Enter the port used to connect to the LDAP server.
LDAP Server Type	Click the search button to select the type of LDAP server: Microsoft, IBM, or Domino. **Note:** If you are configuring LDAP for Oracle Internet Directory, you must add OID to the list of options and select it here. See *Creating a JD Edwards EnterpriseOne LDAP Configuration for OID*.
LDAP Admin ID	Enter the administrator's ID for the LDAP server.
LDAP Admin Password	Enter the administrator's password for the LDAP server.
SSL/TLS Enabled LDAP Server	Select this option if you want to set up Secure Socket Layer (SSL/TLS) communication between EnterpriseOne security kernel and the LDAP server. **Note:** This requires the LDAP server to be configured for SSL/TLS. See *Using LDAP Over SSL/TLS (Release 9.2.1)*.
Role Enabled in LDAP	Select this option if you are managing user-role relationships in LDAP.

Configuring the LDAP Server Settings

Access the LDAP Server Attribute Values form. To do so, on the Available LDAP Configurations form, select a configuration record and then select **Values** from the Row menu.

1. Click the search button in the Enterprise Server Attribute Name column to select the attributes to include in the LDAP server settings.

   After selecting the attributes, you must enter the appropriate LDAP value for the attribute in the LDAP Server Attribute Value column.
2. To configure the standard EnterpriseOne settings for LDAP server, enter values for these attributes:

Attribute	Description
USRSRCHBAS	User search base. Specifies that the system searches for user information at the root of the directory information tree. This value specifies the "container" in which to begin the search. For example, **`USRSRCHBAS=o=jdedwards,c=us`**
USRSRCHFLT	User search filter. Specifies that a search is performed at the base level for the user ID in the LDAP server using the specified criteria. For example, **`USRSRCHFLT=objectclass=inetOrgPerson`** If you do not specify this value, no search filtering occurs.
USRSRCHSCP	User search scope. Specifies the level, or scope, at which the system searches for user information. Valid values are: o **base** The query searches only the value you specified in the USRSRCHBAS setting. o **subtree** This is the default value. The query searches the value in the Search Base field and all entries beneath it. o **onelevel** The query searches only the entries one level down from the value in the Search Base field.
ROLSRCHBAS	Role search base (use only if roles are enabled in LDAP). Specifies that a search is performed at the base level for the UserIDAttri in the LDAP database. For example, **`ROLSRCHBAS=o=jdedwards,c=us`**
ROLSRCHFLT	Role search filter (use only if roles are enabled in LDAP). This specifies that a search is performed at the base level for the role in the LDAP database using the specified criteria. For example, **`ROLSRCHFLT=objectclass=groupOfNames`** If you do not specify this value, no search filtering occurs.

Attribute	Description
ROLSRCHSCP	Role search scope (use only if roles are enabled in LDAP). This specifies the level, or scope, at which the system searches for role information. Valid values are: o **base** The query searches only the value you specified in the ROLSRCHBAS setting. o **subtree** This is the default value. The query searches the value in the Search Base field and all entries beneath it. o **onelevel** The query searches only the entries one level down from the value in the Search Base field.

3. When using Secure Socket Layer (SSL/TLS) with LDAP server, enter values for these attributes:

Attribute	Description
SSLPORT	SSL/TLS Port for the LDAP server. Specifies the SSL/TLS port on the LDAP server.
CERTDBPATH	Dir path for cert7.db (SSL/TLS) For Windows and UNIX: This specifies the directory path to the cert7.db file (SSL/TLS). This file should generally be located in the system\bin32 directory on the Enterprise Server. For IBM i: This specifies the directory path and file name for the cert.kdb file on the IBM i-based, Enterprise Server machine, for example `/QIBM/USERDATA/ICSS/CERT/SERVER/CERT.KDB`. You should use the Digital Certificate Manager (DCM) to verify the location of the certificate for your installation.
CERTDBCLBL	Do not use this attribute. This is for future use only.
CERTDBPSWD	For IBM i only. This is the password to the key database. Specifies the password to the key database (files with a "kdb" extension). The key database is used to store a uniquely identified name, or label, associated with the client private key/certificate pair.
SSLTIMEOUT	For IBM i only. This specifies the time-out value for the SSL connection.

4. If you are using the self-service version of the user profile application for the Manufacturing Sourcing module, enter values for these attributes:

   Note: You cannot use this application to manage LDAP user profiles.

Attribute	Description
USRACNTCTL	User Account Control. Specifies the authority attached when creating a user in Active Directory, for example **USRACNTCTL=512** creates an enabled user in Active Directory only.
USRADDLOC	User Add Location. Specifies the location in LDAP where users will be added, for example **USRADDLOC=O=jdedwards**.
USRCLSHRCY	User Class Hierarchy. Specifies the class hierarchy needed to create a user in LDAP, for example **USRCLSHRCY=top, person, organizationalPerson, inetOrgPerson**.
ROLADDLOC	Role Add Location (use only if roles are enabled in LDAP). Specifies the location in LDAP that contains the user-role relationship, for example **ROLADDLOC=O=jdedwards**.
ROLCLSHRCY	Do not use this attribute. This is for future use only.

Configuring LDAP to EnterpriseOne Enterprise Server Mappings

You can map attributes for users or for user-role relationships depending upon your configuration. If you are entering mappings for user-role relationships, you must also ensure that the LDAP configuration record is enabled for roles.

Access the LDAP Server Mappings form. To do so, on the Available LDAP Configurations form, select **Mappings** from the Row menu.

1. Click the search button in the Enterprise Server Attribute Name column to select the attributes to include in the mappings.

   After selecting the attributes, you must enter the appropriate LDAP value for the attribute in the LDAP Server Actual Attribute column.
2. To configure the LDAP to Enterprise Server mappings:

   For a standard setup, enter values for these attributes:

Attribute	Description
E1USRIDATR	EnterpriseOne User ID Attribute. Specifies the user ID attribute in LDAP that is used for EnterpriseOne users. The system uses this attribute when creating users in LDAP during EnterpriseOne sign-in, for example **E1USRIDATR=cn**.

Attribute	Description
USRSRCHATR	User ID Search Attribute. Specifies the search criteria for the sign-on user ID. This is the value that maps the sign-on user ID in LDAP to the sign-in user ID in EnterpriseOne, for example **USRSRCHATR=cn**. The USRSRCHATR and E1USRIDATR attributes should be mapped to the same value.
ROLNAMEATR	Role Name Attribute (use only if roles are enabled in LDAP). This value maps the role in LDAP to the role in EnterpriseOne, for example **ROLENAMEATR=cn**
ROLSRCHATR	Role Search Attribute (use only if roles are enabled in LDAP). Specifies the search attribute for the role in the LDAP server. The system uses this attribute to search LDAP for a list of roles for a user, for example **ROLSRCHATR=member**.
LANGUAGATR	Language Attribute. Specifies the language attribute used within LDAP, for example **LANGUAGATR=preferredLanguage**

For an EnterpriseOne long user ID configuration, enter values for these attributes:

Attribute	Description
E1USRIDATR	EnterpriseOne User ID Attribute. Specifies the user ID attribute in LDAP that is used for EnterpriseOne users. The system uses this attribute when creating users in LDAP during EnterpriseOne sign-in, for example **E1USRIDATR=uid**.
USRSRCHATR	User ID Search Attribute. Specifies the search criteria for the sign-on user ID. This is the value that maps the sign-on user ID in LDAP to the sign-in user ID in EnterpriseOne, for example **USRSRCHATR=uid**. For a long user ID configuration, the USRSRCHATR and E1USRIDATR attributes should be mapped to different LDAP attributes, for example USRSRCHATR=cn. This is because JDE uses USRSRCHATR to read the long user ID which is used during EnterpriseOne sign-in for a long user ID configuration.
ROLNAMEATR	Role Name Attribute (use only if roles are enabled in LDAP). This value maps the role in LDAP to the role in EnterpriseOne, for example **ROLENAMEATR=cn**
ROLSRCHATR	Role Search Attribute (use only if roles are enabled in LDAP). Specifies the search attribute for the role in the LDAP server. The system uses this attribute to search LDAP for a list of roles for a user, for example **ROLSRCHATR=member**.

Attribute	Description
LANGUAGATR	Language Attribute. Specifies the language attribute used within LDAP, for example **LANGUAGATR=preferredLanguage**

3. If you are using the self-service version of the user profile application for the Manufacturing Sourcing module, enter values for these attributes:

Note: You cannot use this application to manage LDAP user profiles.

Attribute	Description
CMNNAME	Common Name. Specifies the Common Name for a user in LDAP. The system uses this attribute when creating users in LDAP, for example **CMNNAME=cn**
GIVENNAME	Specifies the Given Name for a user in LDAP. It is used when creating users in LDAP, especially in Active Directory, for example **GIVENNAME=givenName**.
SURNAME	Specifies the SUR Name for a user in LDAP. This attribute is used when creating users in LDAP, for example **SURNAME=sn**.
PASSWORD	Specifies the password associated with the account that you specify with the ConnectDN (distinguished name) of the LDAP server.
OBJCLASS	Object Class. Specifies the Object Class attribute for a user in LDAP it is used when creating users in LDAP, for example **OBJCLASS=objectCLASS**.
ACNTCTLATR	Account Control Attribute. Specifies the attribute used in Active Directory for user authority in Active Directory, for example **ACNTCTLATR=userAccountControl**. If the attribute **USRACNTCTL=512** is used in conjunction with **ACNTCTLATR**, the EnterpriseOne API will create an enabled user in Active Directory only.
ACTNAMEATR	Account Name Attribute. Specifies the attribute used only in Active Directory for creating a signon user account, for example **ACNTCTLATR=sAMAccountName**.

Changing the LDAP Configuration Status

After you add an LDAP configuration, by default the configuration is disabled or non-active. You must change the status to active to enable the configuration.

Note: You can have only one active LDAP configuration per port.

Access the Available LDAP Configurations form.

Select a configuration record and then select **Change Status** from the Row menu.

The system changes the status in the Status column to AV (active) or NA (not active).

Enabling LDAP Authentication Mode

In Server Manager, access the Security settings for the Enterprise Server.

In the Security settings, click the **Enable LDAP Authentication** check box to enable security authentication. By default, this setting is cleared or disabled, which disables the LDAP authentication mode.

Modifying the LDAP Default User Profile Settings

This section contains the following topics:

- *Understanding LDAP Default User Profile Settings*
- *Forms Used to Modify the LDAP Default User Profile Settings*
- *Reviewing the Current LDAP Default Settings*
- *Modifying the Default User Profile Settings for LDAP*
- *Modifying the Default Role Relationships for LDAP*
- *Modifying the Default User Security Settings for LDAP*

Understanding LDAP Default User Profile Settings

You must configure and review the default LDAP user profile settings that are in the EnterpriseOne database. The system requires the default settings for user profile synchronization. These values are synchronized from LDAP to EnterpriseOne by the LDAP synchronization mechanisms (security kernel and batch report). The default user profile settings are written to the F0092 table.

Note: You must add the default LDAP user profile settings before enabling LDAP authentication in the jde.ini file of the EnterpriseOne security server.

The Configuring LDAP Defaults form shows whether the following items exist for the default user:

- User profile
- Role relationships
- Data source/system user

  Note: Changes made in this application can affect almost all EnterpriseOne users when synchronizing data from LDAP to the EnterpriseOne database.

Forms Used to Modify the LDAP Default User Profile Settings

Form Name	FormID	Navigation	Usage
Configure LDAP Defaults	W0092M	In Solution Explorer, from the System Administration Tools menu (GH9011), select Security Maintenance, Security Maintenance Advanced and Technical Operations, Configure LDAP Defaults.	Review the current LDAP default settings.
User Profile Revisions	W0092A	On the Configure LDAP Defaults form, click the User Profile link.	Modify the default user profile settings for LDAP.
Work with Role Relationships	W95921C	On the Configure LDAP Defaults form, click the Role Relationships link.	Add roles to the default user.
Work With User Security	W98OWSECE	On the Configure LDAP Defaults form, click the Data Source/System User link.	Add or modify the data source or system user settings.
Data Source Revisions	W98OWSECH	On the Work With User Security form, select a security record and then click Select.	Assign a different system user to the data source.
Security Revisions	W98OWSECB	On the Work With User Security form, click Add.	Add an additional data source.

Reviewing the Current LDAP Default Settings

Access the Configure LDAP Defaults form.

> **Note:** All user values are assigned per user ID the first time, and the first time only, that a user signs in. During this initial sign-in, the values are synchronized from LDAP to the EnterpriseOne database. The default role relationship is synchronized only if roles are managed by EnterpriseOne.

LDAP Authentication

Indicates whether LDAP authentication is enabled or disabled.

Role Management

Indicates whether roles are managed by LDAP. You can enable EnterpriseOne to manage roles in LDAP through the P95928 application.

See *Creating an LDAP Configuration*.

User Profile

Indicates whether a default user profile exists within the EnterpriseOne database. Click this link to modify the default user profile settings.

See *Modifying the LDAP Default User Profile Settings*.

Role Relationships

Indicates whether a default role relationship exists. If LDAP authentication is enabled, and if user-role relationships are set to be managed by LDAP, then this option is disabled. This means that the system does not use the default user-role relationship when synchronizing users from LDAP to the EnterpriseOne database.

To revise the default role relationship, see *Modifying the Default Role Relationships for LDAP*.

Data Source/System User

Indicates whether a default data source or system user exists. Click this link to add or change the data source or system user.

See *Modifying the Default User Security Settings for LDAP*.

Modifying the Default User Profile Settings for LDAP

Access the User Profile Revisions form. To do so, on the Configure LDAP Defaults form, click the User Profile link.

Modify the appropriate fields.

> **Note:** The User ID field always contains the default user ID for the LDAP system. This field is read only.

Modifying the Default Role Relationships for LDAP

Access the Work With Role Relationships form. To do so, on the Configure LDAP Defaults form, click the Role Relationships link.

> **Note:** If LDAP authentication is enabled and user-role relationships are being managed by LDAP, then this option is disabled. This means that user-role relationship functionality from within EnterpriseOne is disabled.

On the Work With Role Relationships form, you can highlight a role in either the Assigned Roles or Available Roles menus, and then click the appropriate directional arrow button to add or remove the role for the default user.

> **Note:** These values are only synchronized between EnterpriseOne and LDAP if the role is being managed by EnterpriseOne.

Modifying the Default User Security Settings for LDAP

Access the Configure LDAP Defaults form.

1. In the Configure Defaults area, click the Data Source/System User link.
   If the default data source or system user does not exist, the Security Revisions form appears.
2. On the Security Revisions form, complete the System User field to add or change the data source or system user.
   If the default data source is defined, the Work With User Security form appears.
3. To assign a different system user to the data source, on the Work With User Security form, select the security record and then click **Select**.
4. On Data Source Revisions, click the search button in the System User field to assign a different system user.
5. To add an additional data source, on the Work With User Security form, click **Add**.
6. On the Security Revisions form, complete the fields as appropriate.

Using LDAP Bulk Synchronization (R9200040)

This section provides an overview of LDAP bulk synchronization and discusses how to run the LDAP Bulk Synchronization batch process (R9200040).

Understanding LDAP Batch Synchronization

The LDAP server contains user profile data for multiple users. This data must also exist in the EnterpriseOne database server. The LDAP Bulk Synchronization batch process (R9200040) enables you to perform bulk synchronization of user profile records from the LDAP server to the EnterpriseOne database. Therefore, this report is beneficial because it populates data that is required for EnterpriseOne functionality.

> **Note:** If the EnterpriseOne database contains user profile records that are not in the LDAP server, this data cannot be synchronized from EnterpriseOne to the LDAP server using the R9200040 batch process. EnterpriseOne does not provide a utility to perform this function.

Running the report synchronizes user profile data obtained from the LDAP server to the following EnterpriseOne database tables:

Table	Description
F0092	Library List User
F0092L	Long User ID to Short User ID
F00921	User Display Preferences
F98OWSEC	Security settings

Table	Description
F95921	Role Relationship
F0093	Library List Control
F00922	User Display Preferences Tag File
F00924	User Install Package
F00926	Anonymous User Access Table
F9005	Variant Description - Control Tables
F9006	Variant Detail - Control Tables

Example: LDAP Bulk Synchronization (R9200040)

The following example shows the PDF output of the R9200040 batch process. Note that if the data on the LDAP server is already the same as the corresponding data on the EnterpriseOne database server, the report lists the affected tables and shows a zero record synchronization, which indicates the data exists, but is identical.

Worldwide Company

Synchronize the LDAP and EnterpriseOne Database

Table Name	Records Added	Records Deleted	Records Failed	Synchronization Status
F0092	17	219	0	Successful
F00921	17	219	0	Successful
F98OWSEC	34	148	0	Successful
F95921	43	272	0	Successful
F9312	0	0	0	Successful
F0093	0	133	0	Successful
F00922	0	13	0	Successful
F00924	0	3	0	Successful

Running the LDAP Bulk Synchronization Batch Process (R9200040)

Access the Batch Versions application (P98305). To do so, enter `P98305` in the Fast Path.

1. On the Work With Batch Versions – Available Versions form, enter `R9200040` in the Batch Application field and click Select.
2. On the Version Prompting form, click **Submit**.

Using LDAP Over SSL/TLS (Release 9.2.1)

This section provides an overview on how to enable LDAP authentication over Secure Socket Layer (SSL/TLS) and discusses how to:

- Enable LDAP authentication over SSL/TLS for Windows and UNIX.
- Enable LDAP authentication over SSL/TLS for IBM i.

Understanding LDAP with SSL/TLS

You can establish a secure LDAP connection between the EnterpriseOne Server and the LDAP server.

LDAP Authentication Over SSL/TLS for Windows and UNIX

The EnterpriseOne server uses Netscape's certificate database, cert7.db or cert9.db. You use the "certutil" utility, found in \system \bin32 or \system\bin64 to create the cert9 certificate database. The "certutil" utility will only create the cert9.db, but runtime is backward compatible with cert7.db.

> **Note:** As of Tools Release 9.2.5.3, Mozilla Network Security Services (NSS) does not support the AIX platform. Because of this limitation, you will not be able to use the certutil tool present in this path: \system \bin32 or \system \bin64. The EnterpriseOne server uses Netscape's certificate database, cert7.db or cert9.db. You can obtain the cert7.db or cert9.db certificates using the PKCS utilities distributed by Netscape.

For Windows and UNIX, establishing the secure connection between the EnterpriseOne application server and the LDAP server requires these items:

- Cert7.db / cert9.db certificate database from Netscape.
- A server certificate for the LDAP server.
- The trusted root certificate from the certificate authority (CA) that issues the server certificate.

LDAP Authentication Over SSL for IBM i

The EnterpriseOne server uses IBM certificate database (.kdb) to store certificates on IBM i. You can create a certificate database on IBM i using Digital Certificate Manager.

For IBM i, establishing a secure connection between the EnterpriseOne application server and the LDAP server requires these items:

- IBM Certificate store (.kdb) certificate database.
- A server certificate for the LDAP server.
- The trusted root certificate from the certificate authority (CA) that issues the server certificate.

Enabling LDAP Authentication Over SSL/TLS for Windows and UNIX

To enable LDAP authentication over SSL/TLS for Windows or UNIX:

1. Follow the documentation for your directory server to add the server certificate to the directory server.
2. Using Netscape's PKCS Utilities, add the CA's trusted root certificate to the cert7.db certificate database.
3. Enable SSL/TLS for the LDAP configuration using the LDAP Server Configuration Workbench application.
4. Specify the SSL/TLS parameters.

   See *Configuring the LDAP Server Settings*.
5. Restart the EnterpriseOne server.

Enabling LDAP Authentication Over SSL for IBM i

To enable LDAP authentication over SSL for IBM i:

1. Follow the documentation for your directory server to add the server certificate to the directory server.
2. Use Digital Certificate Manager to add and export the CA's trusted root certificate to the certificate database (.kdb file).
3. Enable the SSL for the LDAP configuration using the LDAP Server Configuration Workbench application.
4. Specify the SSL parameters.

   See *Configuring the LDAP Server Settings*.
5. Restart the EnterpriseOne server.

Exporting User Data to the LDAP Server

This section contains the following topics:

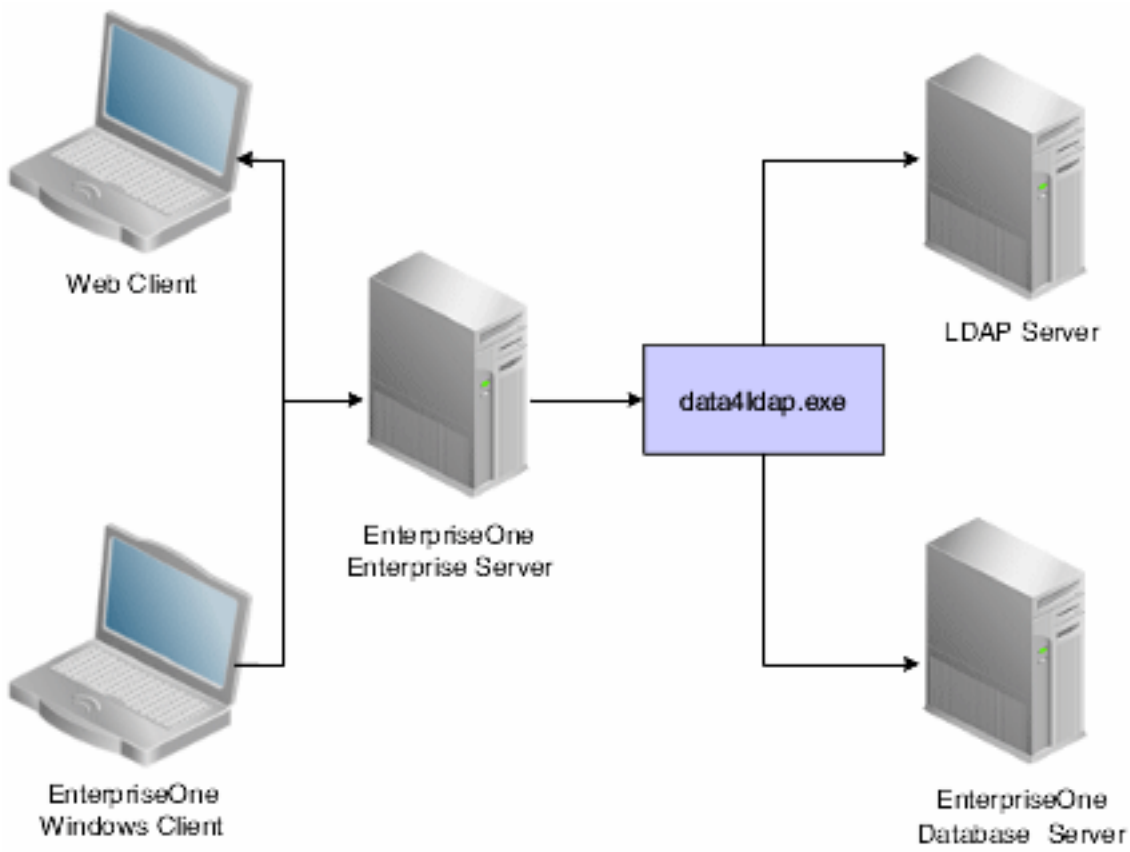
Understanding the data4ldap Utility

The data4ldap utility automates the process of uploading EnterpriseOne user data to the LDAP server. The EnterpriseOne user data includes:

- EnterpriseOne user ID
- Password
- Language attribute
- User-role relationship

Note: data4ldap does not export passwords.

If you do not use this utility, you would have to populate the repository manually, which can lead to data being entered incorrectly. This illustration shows the data4ldap.exe utility uploading the EnterpriseOne user data to the LDAP server.



The Language attribute is uploaded only for those EnterpriseOne users who are specifically assigned a language. By default, no language is assigned to a user when a user is added to EnterpriseOne. In such a case, no language is available for the particular user in the LDAP server. For example, if User 1 is assigned language E and User 2 is not assigned to any language, the language attribute is uploaded to the LDAP server only for User 1 and not for User 2.

Expired EnterpriseOne users and roles are also exported to the LDAP server. If an EnterpriseOne user record does not exist in the table F98OWSEC, then the particular user would not be exported to the LDAP server.

Prerequisites

Before you use the data4ldap utility, you must:

- Use the LDAP Server Configuration Workbench application (P95928) to map these items:

  See *Enabling LDAP Support in JD Edwards EnterpriseOne*.

  - User Search Attribute
  - User Search Base
  - User Class Hierarchy
  - Role Search Attribute
  - Role Name Attribute
  - Role Search Base
  - Role Class Hierarchy
  - Object Class
  - Password

    If these fields are left blank, no operation is performed; the utility generates an appropriate error message and exits.
- For Microsoft Active Directory, map the following attributes in addition to the above mentioned ones:
  - User Account Control
  - Account Control Attribute
  - Account Name Attribute
- Use the LDAP Administrator user ID and password. If either the LDAP Administrator user ID or password field is blank in P95928, the utility cannot export EnterpriseOne user-role data to the LDAP server. It will generate an error message and exit.
- Disable the password policies of the LDAP server. For further information, refer to the documentation of the directory server that you are using for the LDAP server or contact your LDAP Administrator.

Granting Access to the data4ldap Utility

The data4ldap utility involves working with secured data, so you must ensure that only authorized users are able to access and run it. Use the External Calls Security form in the Security Workbench application (P00950) to grant a user or administrator access to this utility.

See *Adding External Call Security*.

Configuring Parameters Required to Run the data4ldap Utility

The data4ldap utility can run only on the Enterprise Server and not on the client.

To run the data4ldap utility, you must configure these parameters:

```
data4ldap <UserID> <Environment> <Role> <IsRoleIncluded (*YES/*NO)> <IsOverwrite#
Allowed (*YES/*NO)>
```

Parameter	Description
UserID	Enter a valid EnterpriseOne user ID that has been granted access to the utility from External Call Security.
Environment	Enter a valid EnterpriseOne environment.
Role	Enter a valid EnterpriseOne role.
IsRoleIncluded	Specify whether or not EnterpriseOne role information is included in the export to the LDAP server. Enter *YES to export role information. Enter *NO to not export role information.
IsOverwriteAllowed	Determine whether you want to override the LDAP server entries with the EnterpriseOne user-role data: Enter *YES to overwrite the LDAP server entries with the EnterpriseOne user-role data. Enter *NO if you do not want to overwrite the LDAP server entries with the EnterpriseOne user-role data.

Note: The IsOverwriteAllowed parameter is used in case the LDAP server already contains user data that is identical to EnterpriseOne user data. In this case, you have the option to overwrite the existing LDAP server user IDs with the current EnterpriseOne user IDs. The value of IsOverwriteAllowed parameter is valid only for user data (common name, language, and given name whichever is configured through the application P95928) and not for user-role relationship data.

Running the data4ldap Utility on Windows

In the command prompt, navigate to Enterprise Server System\bin32.

1. Enter the valid parameters. For example:

   ```
   data4ldap JDE DV812 *ALL *YES *YES
   ```
2. Press Enter.

   The utility prompts for User – Password.
3. Enter the password for the EnterpriseOne account.

Running the data4ldap Utility on Unix or Linux

In the command prompt, navigate to Enterprise Server System\bin32.

1. Enter the valid parameters. For example:

   ```
   data4ldap JDE DV812 *ALL *YES *YES
   ```
2. Press Enter.

   The utility prompts for User – Password.
3. Enter the password for the EnterpriseOne account.

Running the data4ldap utility on IBM i

Access the IBM i command prompt.

1. Under "Selection or command," type **data4ldap** and press F4.

   Some default values that are editable appear on the screen.
2. Enter the valid parameters, for example:

   ```
   data4ldap JDE Password DV812 *ALL *YES *YES
   ```
3. Press Enter.

Scenarios for Uploading Users to the LDAP Server

This section discusses the following scenarios for uploading users to the LDAP server:

- data4ldap JDE DV812 *ALL *NO *YES
- data4ldap JDE DV812 *ALL *YES *YES
- data4ldap JDE DV812 *ALL *YES *NO
- data4ldap JDE DV812 *ALL *NO *NO

data4ldap JDE DV812 *ALL *NO *YES

All EnterpriseOne users are uploaded to the LDAP server and existing LDAP user data is overwritten. However, EnterpriseOne user-role relationship data is neither uploaded nor overwritten in the LDAP server.

data4ldap JDE DV812 *ALL *YES *YES

All EnterpriseOne user and user-role relationship data is uploaded to the LDAP server. The existing LDAP user data and LDAP role-relationship data is overwritten.

data4ldap JDE DV812 *ALL *YES *NO

All EnterpriseOne users who do not exist in the LDAP server are uploaded to the LDAP server. The existing LDAP users are not be overwritten.

All EnterpriseOne user-role relationship data is uploaded to the LDAP server and the existing LDAP role-relationship data is overwritten.

data4ldap JDE DV812 *ALL *NO *NO

All EnterpriseOne users who do not exist in the LDAP server are uploaded to the LDAP server, and the existing LDAP users are not overwritten.

However, EnterpriseOne user-role relationship data would neither be uploaded nor overwritten in the LDAP Server.

LDAP Server Behavior

This section provides information about LDAP server and:

- Tree Delete control
- Microsoft Active Directory

Tree Delete Control

IBM Directory Server (IDS) and Microsoft Active Directory support Tree Delete Control. The Tree Delete Control extends the delete operation and allows the removal of sub trees within a directory using a single delete request.

It is always recommended that if the Role data are managed by the LDAP server, include the Role data (isRoleIncluded = *YES) while choosing the Overwrite option (isOverwriteAllowed = *YES).

For more details on Tree Delete Control, see:

http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzahy/rzahycontrols.htm

Note: Oracle Internet Directory (OID) does not support Tree Delete Control.

Microsoft Active Directory

Microsoft Active Directory uses "inetOrgPerson" and a user password can be stored in the Active Directory attribute called "userPassword". However, Microsoft Active Directory must be configured to store a user password in the "userPassword" attribute. It can be configured by setting the 9th bit of dsHeuristics value. It is located in CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=domain. object. The value should look like this: 000000001. For more information, refer to Microsoft documentation.

http://msdn.microsoft.com/en-us/library/cc223249.aspx

http://msdn.microsoft.com/en-us/library/cc223560.aspx

Consider the following items when using Microsoft Active Directory:

- EnterpriseOne application P95928 should be configured accordingly for "InetOrgPerson" and "userPassword".
- For Microsoft Active Directory, the EnterpriseOne data can be dynamically uploaded only over a SSL/TLS connection. This is due to the Microsoft Active Directory restriction.
- Microsoft Active Directory user-password authentication is case sensitive. The user information uploaded from EnterpriseOne does not include user passwords. Therefore, passwords must be entered by an administrator or end users using the applicable LDAP tool. The passwords are stored in the case in which they are entered.

During sign-in, other LDAP servers ignore the case of the supplied password, whereas Microsoft Active Directory fails to authenticate a user if the supplied password is not in the correct case.

- In case a user does not get uploaded to Microsoft Active Directory, all of the roles assigned to the particular user would also not be uploaded to Microsoft Active Directory. This restriction is valid only for Microsoft Active Directory and not for OID / IDS.

Setting Up Microsoft Active Directory Server

The Microsoft Active Directory Server can be used with EnterpriseOne only if it is enabled for using SSL.

To set up the Microsoft Active Directory Server and enable it for using SSL, perform the following steps:

> **Note:** Make sure that you have the administrator password for the server. After you install the Active Directory and start the server, you cannot log in if you do not have the administrator password.

1. Install **Active Directory Domain Services** and promote this server to a domain controller by following the steps explained in the *Installing AD DS by using Server Manager* section.
2. On the Server Manager page, click the **Manage** menu and select **Add Roles and Features**.
3. Install Active Directory Certificate Services by selecting the **Certificate Authority** option.
4. To configure the CA Certificate, click **Create Active Directory Domain Services.**
5. Retain the default values on all the windows except in the **Cryptography for CA** window. In the Cryptography for CA window, select the value for the **Hash Algorithm** as **SHA256** and click **Next**.
6. Click the **Configure** button on the last window to complete configuring the CA Certificate.
7. Install the latest Windows Security Updates (dated March 10, 2020).

For more information see:

1. *LDAP channel binding and signing for Microsoft Active Directory*
2. *LDAP signing*

15 Setting Up JD Edwards EnterpriseOne Single Sign-On

JD Edwards EnterpriseOne Single Sign-On Overview

JD Edwards EnterpriseOne single sign-on enables users that are signed in to JD Edwards Collaborative Portal to access EnterpriseOne applications without re-entering a user ID and password. Single sign-on increases the security for the EnterpriseOne system since passwords are no longer passing between different sub-systems in EnterpriseOne.

Note: EnterpriseOne does not support single sign-on between EnterpriseOne applications and third-party applications.

Authenticate Tokens

EnterpriseOne uses an authenticate token to achieve single sign-on. The authenticate token contains criteria that grants access to an EnterpriseOne application from JD Edwards Collaborative Portal. When a user signs on to either system, after successful authentication, the system generates an authenticate token. When a user accesses an EnterpriseOne application, the system uses the generated token to validate the user against the EnterpriseOne security server. As a result, the user does not have to manually sign on to the system again.

When a user signs on to either system, an authenticate token is generated after successful authentication. When the user accesses an EnterpriseOne application, the system uses the generated token to validate the user against the EnterpriseOne security server. As a result, the user does not have to manually sign on to the system again.

For security purposes, all authenticate tokens expire after a certain period of time and contain a digital signature that ensures the token cannot be tampered with.

An authenticate token contains these properties:

Property	Description
User ID	The user ID that the server issued the token for. When the browser submits this token for single sign-on, this is the user that the application server signs in to the system.
Language Code	The language code of a user. When the system uses a token for single sign-on, it sets the language code for the session based on this value.
Date and Time Issued	The date and time the token was first issued. The system uses this field to enforce a time-out interval for the single sign-on token. Any application server that accepts tokens for sign-on compares this value against the amount of time set in the application server to accept tokens. The value is in Greenwich Mean Time (GMT) so it does not matter which time zone the application server is in. **Note:** The system date and time is used to validate the expiration of a token. Changing these values on the server may expose a potential security risk.
Issuing Node Name	The name of the machine that issued the token.

Property	Description
Signature	A digital signature that the application server (node) uses to validate the token for single sign-on by ensuring that the token has not been tampered with since it was originally issued. The machine issuing the token generates the signature by concatenating the contents of the token (all the fields that appear in this table) with the message node password for the local node. Then the system hashes the resulting string using the SHA1 hash algorithm. For example ("+" means concatenation), signature = SHA1_Hash (UserID + Lang + Date Time issued + Issuing Node Name+ Issuing Node Password) There is only one way to derive the 160 bits of data that make up the signature, and that is by hashing exactly the same User ID, Language, Date Time, Issuing System, and node password.

Nodes

A node is a machine that can generate or validate an authenticate token. The node contains properties that you set to control security and specify parameters for which tokens the node will accept. The system stores the node properties in the database or the jde.ini files, depending on your particular setup.

Each node contains these properties:

Property	Description
Node name	A logical name associated with this node. The length of the node name cannot exceed 15 characters.
Node password	Each node has a password which is known only by the system administrator. It serves as a key to ensure that the token does not get tampered with after it is generated.
Physical machine name	The physical machine name in which the node resides.
Trusted nodes list	This property contains the list of nodes that can be trusted by this node. For security purposes, only tokens that are generated by predefined machines can be accepted. These predefined machines are called trusted nodes. The trusted node is one-way, for example if you set up node A to trust node B, it does not mean that node B trusts node A.
Token lifetime properties	When validating a token, the node checks the time the token was issued against the amount of time that you set in the token lifetime properties. For example, if you set the token lifetime for six hours, and the node receives a token that was originally issued seven hours prior, the node will not accept the token. You can use these two properties to specify the token lifetime: • Regular token lifetime This property specifies the expiration time for a regular token. A regular token gives a user the authority to run a regular short-run process, such as a business function. The default value for this property is 12 hours.

Property	Description
	• Extended token lifetime This property specifies the expiration time for an extended token. An extended token gives a user the authority to run a long-run process, such as a UBE, after it is issued. The default value for this property is 30 days.

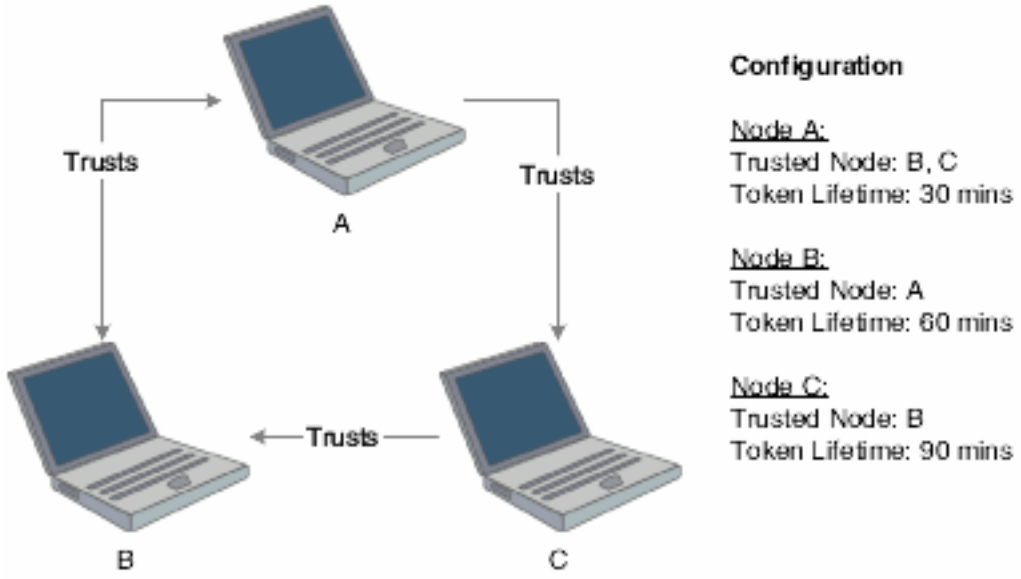
Note: On the IBM i platform, GMT time calculation does not take into account daylight savings time. Consequently, there can be a one hour difference in GMT time calculation between tokens generated on IBM i and Windows platforms. If you set the token timeout values as 12 hours (the default) or longer, you will notice this issue in sessions running for longer than 11 hours. If you set the token timeout values as less than one hour, then the tokens generated on Windows will automatically expire on IBM i. To resolve this issue, on the IBM i server, you should change the QUTCOFFSET value manually whenever there is a change in daylight savings time to ensure proper calculation of GMT time.

How a Node Validates an Authenticate Token

The node validates an authenticate token by checking whether:

- The token signature has been changed.
- The token is expired.
- The token is generated by a trusted node.

This diagram is an example of token validation in a multiple node setup:



According to this configuration, the following tokens are validated by a node:

- Node A validates tokens generated by node B and node C if received less than 30 minutes from generation.
- Node B validates tokens generated by node A if received less than 60 minutes from generation.
- Node C validates tokens generated by node B if received less than 90 minutes from generation.

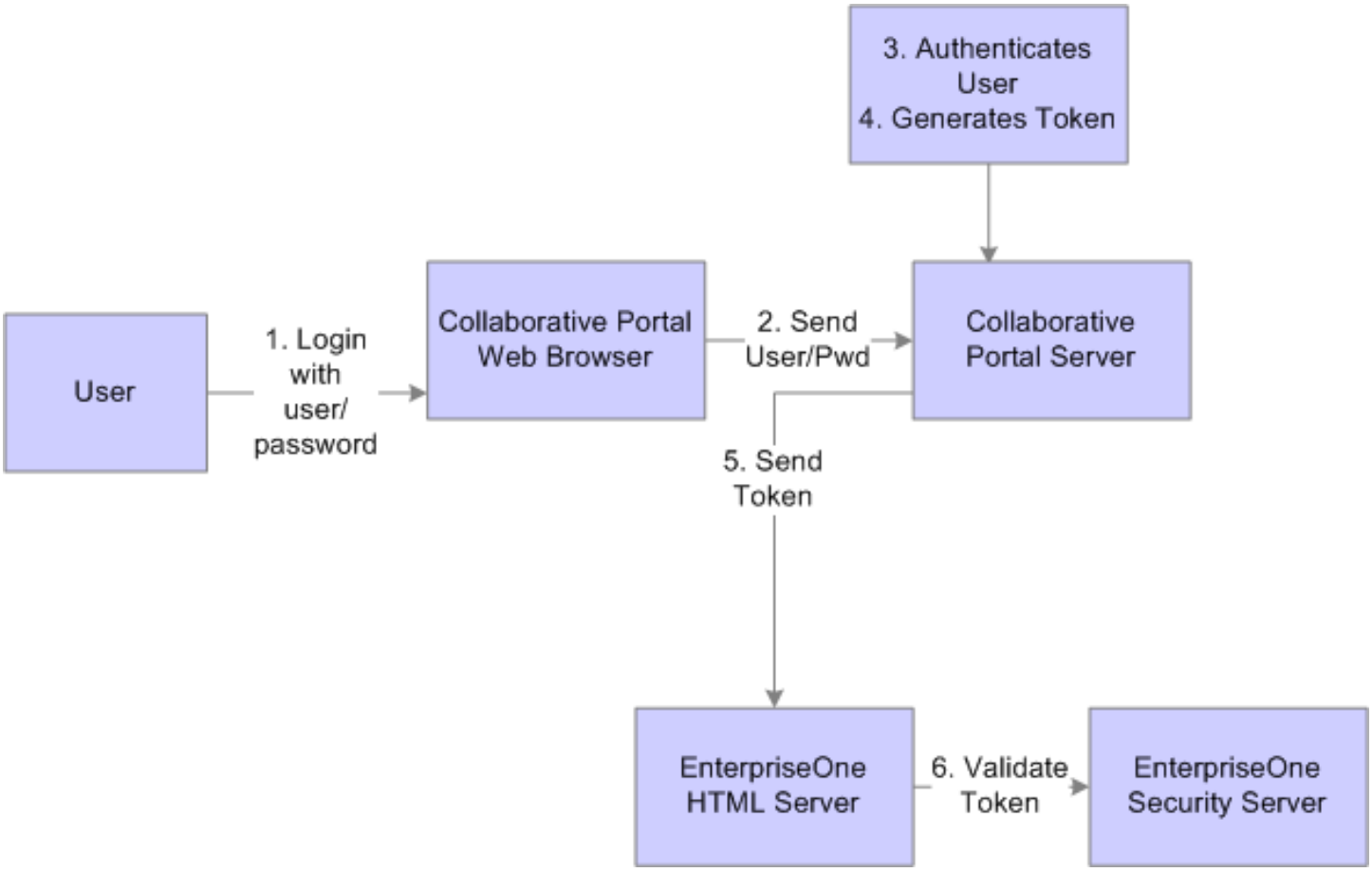
The following tokens are not validated by a node:

- Node B cannot accept a token generated by node C, even though node C trusts node B.
- A node will not accept a token if the time between its generation and reception by the node is greater than the token lifetime set for that node. For example, node A cannot accept a token from node B if the token was generated more than 30 minutes prior to being received by node A.

> **Note:** No node will accept a token if its signature has been changed. The system verifies this by comparing the token signature and the hash value of the token body.

Single Sign-On Scenario: Launching an EnterpriseOne Application from JD Edwards Collaborative Portal

The illustration and steps in this section explain how single sign-on works when a user signs in to JD Edwards Collaborative Portal and launches an EnterpriseOne application:



1. The user signs in to JD Edwards Collaborative Portal through a web browser using an EnterpriseOne user ID and password.
2. The system sends the user ID and password to the JD Edwards Collaborative Portal.
3. JD Edwards Collaborative Portal authenticates the user ID and password against either LDAP, EnterpriseOne tables, or WebSphere security.
4. A token is generated for the user ID.
5. When single sign-on is required for EnterpriseOne, the token is sent to either a HTML Server or a EnterpriseOne application server.
6. The EnterpriseOne security server validates the token and grants access to the EnterpriseOne application.

Understanding the Default Settings for the Single Sign-On Node Configuration

By default, when there is no configuration table specifications in the system and no configurations in the jde.ini file, the security server uses these settings for node information:

Setting	Description
Logical Node Name	_GLOBALNODE
Physical machine name	N/A (The default settings are all the same independent of the physical machine that it is residue in.)
Regular token timeout	12 hours
Extended token timeout	30 days
Trusted node	_GLOBALNODE

As a result, the EnterpriseOne system will generate a token with node name _GLOBALNODE, and it will only accept a token with node name _GLOBALNODE.

Note: Using default settings may expose a potential security risk. Thus, it is highly recommend to overwrite the single sign-on settings using the single sign-on configuration applications discussed in this section.

Setting Up a Node Configuration

This section provides an overview of the single sign-on configurations and discusses how to:

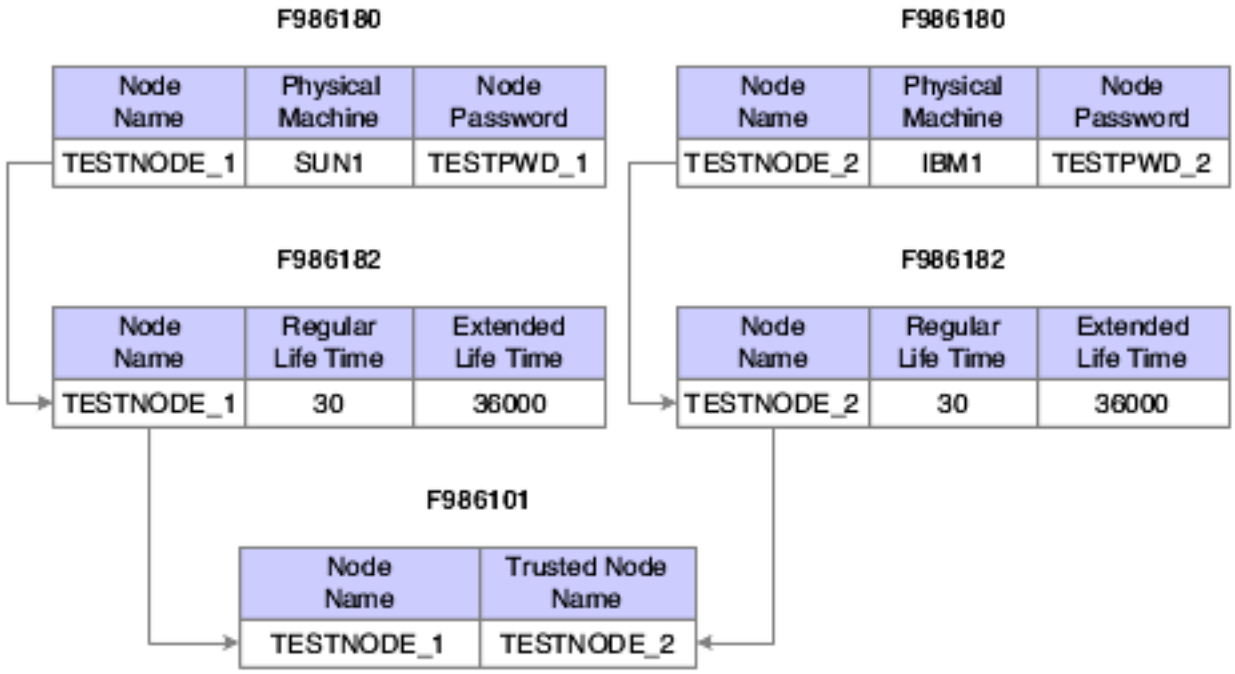
- Add a node configuration.
- Revise a node configuration
- Change the status of a node.
- Delete a node configuration.

Understanding Single Sign-On Configurations and Their Relationships

In EnterpriseOne, the node configurations are stored in a database. The node lifetime configuration is the configuration for the existing node, and the nodes in the trusted node configuration must have an existing node that has the lifetime configurations. The node properties are stored in these three database tables:

- Node Configuration Table (F986180). This table contains the information of a node in the single sign-on environment, such as the node name, description, machine name, node status (active/inactive), and the password.
- Node Lifetime Configuration Table (F986182): This table contains the lifetime information for an existing node. The node lifetime configuration information, such as the node name, regular token lifetime, and extended token lifetime.
- Trusted Node Configuration Table (F986181): This table contains the trust relationship between two nodes.

This diagram shows the relationship among these tables:



This configuration requires that you configure the single sign-on settings in this order:

1. Set up node information.
2. Set up node lifetime.
3. Establish the trust between nodes.

You should delete the single sign-on settings in this order:

1. Delete the trusted node relationship.
2. Delete the node lifetime.
3. Delete the node information.

Alternatively, you can delete the node information directly by deleting the node record in the F986180 table. The system will automatically delete the record's corresponding entries in the Node Lifetime (F986181) and Trusted Node (F986182) tables.

Adding a Node Configuration

Access the SSO Environment Configuration Tools form. In JD Edwards Solution Explorer, select System Administration Tools (GH9011), Security Maintenance, Security Maintenance Advanced and Technical Operations, and then double-click SSO Environment Configuration Tools.

1. Click the **Single Signon Node Configuration** link.
2. On the Work With Node Configuration form, click **Add**.
3. On the SSO Node Configuration Revisions form, complete these fields:

Field	Description
Node Name	Enter a logical name associated with this node. The length of the node name cannot exceed 15 characters.

Field	Description
Node Description	Enter a description of the node.
Machine Name	Enter the physical machine name where the node resides.
Node Status	Specify whether the node is active or inactive.
Node Password	Enter a password for the node. The password ensures that tokens that are generated from the node do not get tampered with.
Verify Node Password	Re-enter the password.

Revising a Node Configuration

Access the Work With Node Configuration form.

1. Select a node and then click **Select**.
2. On SSO Node Configuration Revision, modify the appropriate fields.

Changing the Status of a Node

Access the Work With Node Configuration form.

Select the node and then from the Row menu, select Active/Inactive to change the status of the node.

Deleting a Node Configuration

Deleting an existing node configuration results in the removal of its lifetime configuration and trusted node configuration records in F986181 and F986182 respectively.

Access the Work With Node Configuration form.

1. Select the node that you want to delete and click **Delete**.

   A warning message appears informing you of the corresponding records that are deleted when you delete a node configuration.
2. Click **OK** to delete the node configuration.

Configuring EnterpriseOne HTML Server for JSON Web Token (JWT) (Release 9.2.3.2)

This section discusses how to:

- Understand JSON Web Token Authentication.
- Configure EnterpriseOne Server Trust of the HTML Server.
- Add an existing certificate to a new keystore.
- Configure HTML Server with a certificate.

Understanding JSON Web Token Authentication

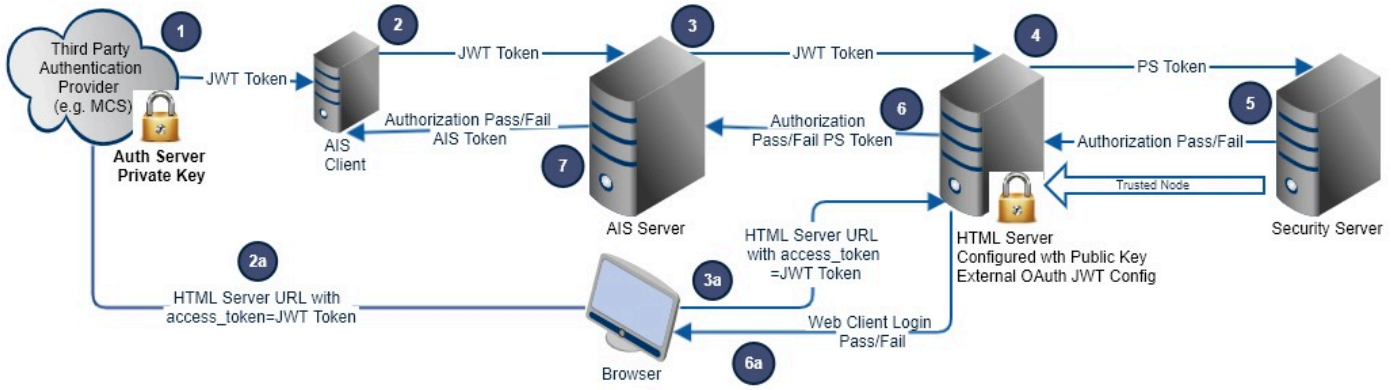
To provide single sign on access using JD Edwards EnterpriseOne and any JWT producing authority, including Oracle Mobile Cloud Service, you need to configure the EnterpriseOne Server trust of the HTML Server, add an existing certificate to a new keystore, and then configure the HTML Server with a certificate. These configurations allow you to establish a trust relationship between a token provider (such as Mobile Cloud Service) and an EnterpriseOne AIS Server and HTML Server.

JWT Authentication Flow

For authentication with a JWT, the following must take place:

- The public key certificate used for token generation by the third party must be provided.
- You must store this certificate in a secure PKCS12 keystore (.p12) and upload it to the EnterpriseOne HTML Server.
- You must configure the EnterpriseOne HTML Server with the keystore name, keystore password, and certificate alias.
- Principal passed in the JWT must match the EnterpriseOne user ID.
- You must configure the EnterpriseOne HTML Server as a trusted node through a single sign-on trust configuration.

The following image shows the authentication flow in an environment in which JWT is used for authentication.



The following steps describe the AIS authentication flows:

1. A third party authentication provider generates a JWT with private key.
2. The JWT is sent in the Bearer header of an AIS token request. (Stateless requests are also supported).
3. The JWT is forwarded to the EnterpriseOne HTML Server by the AIS Server in the Bearer if login is required, and the AIS Server is configured to allow a JWT.
4. The JWT is validated against the public key, the token timeout is validated, and the principal (user) is extracted from the JWT payload. A PSToken is generated for that user and sent for authorization by the Security Server (EnterpriseOne Enterprise Server).
5. The Security Server checks the PS token with SSO node trust, and then an authorization response is returned to the EnterpriseOne HTML Server.
6. The authorization response is returned to the AIS Server. The PS Token is included in the response.
7. The authorization response is returned to the AIS client (third-party). If passed, for a token request the response includes an AIS token.

(Release 9.2.5.4 and later) The following steps describe the HTML authentication flows:

1. A third party authentication provider generates a JWT with private key.

2a. The JWT is sent in the access token URL parameter of the HTML server (E1Web Client) URL.

3a. The JWT is forwarded to the EnterpriseOne HTML by the browser through the URL parameter.

4. The JWT is validated against the public key, the token timeout is validated, and the principal (user) is extracted from the JWT payload. A PSToken is generated for that user and sent for authorization by the Security Server (EnterpriseOne Enterprise Server).

5. The Security Server checks the PS token with SSO node trust, and then an authorization response is returned to the EnterpriseOne HTML Server.

6a. The authorization response is returned to the browser, and user is logged in to the Web Client or the login has failed.

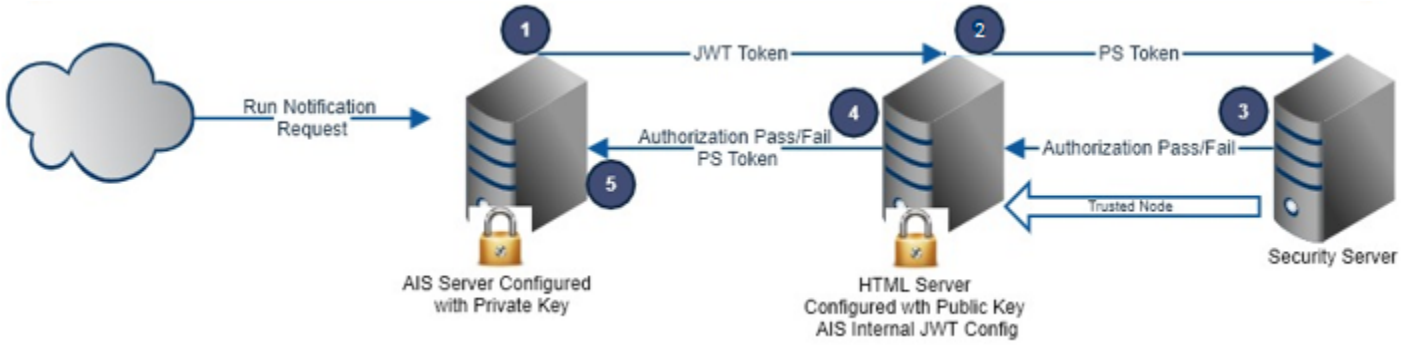
7. The authorization response is returned to the AIS client (third-party). If passed, for a token request the response includes an AIS token.

JWT Internal Flow

For authentication with a JWT, the following must take place:

- You must configure the private key certificate that is used for token generation on the AIS Server. It is initially configured with the Demo Certificate.
- You must configure the public key certificate used for token validation on the HTML Server.
- You must store the certificate in a secure PKCS 12 keystore (.p12) and upload it to the HTML Server.
- You must configure the EnterpriseOne HTML Server as a trusted node through the single sign-on trust configuration.

The following image shows the internal authentication flow in an environment in which JWT is used for authentication.



The following steps describe the internal authentication flow:

1. A JWT is generated for each subscriber (with the subscriber user ID) and is passed to the JTML Server to establish a session.
2. The JWT is validated against the public key, the token timeout is validated, and the principal (user) is extracted from the JWT payload. A PS Token is generated for that user and sent for authorization by the Security Server (EnterpriseOne Enterprise Server).
3. The Security Server checks the PS token with SSO node trust, and then an authorization response is returned to the EnterpriseOne HTML Server.
4. The authorization response is returned to the AIS Server. The PS Token is included in the response.
5. The AIS Server uses that subscriber's session to execute the defined notification and then logs out.

Accessing the Web Client with JSON Web Tokens (Tools Release 9.2.5.4)

Starting with Tools Release 9.2.5.4, you can use JWT to access the EnterpriseOne Web Client and Orchestrator Studio and establish a session with a browser. To do this, you must include JWT in the URL by using the following `access_token` parameter:

```
https://<MyE1HTMLServer>/jde/E1Menu.maf?access_token=eyJ4NXQiOiJxd0V
```

```
https://<MyAISServer>/studio/studio.html?access_token=eyJ4NXQiOiJxd0V
```

Additionally, you can use the JWT with an application shortcut (Parameterized URL) as shown in this example:

```
https://<MyE1HTMLServer>/jde/ShortcutLauncher?OID=P01012_W01012B_ZJDE0001& access_token=eyJ4NXQiOiJxd0V
```

Note: It is recommended by Oracle that single-use JWT are used for this purpose.

You must include the following assertions in your JWT payload to ensure that single-use JWT are used:

- **jti** : This assertion must be unique for every JWT.
- **at_use_nbr**: The value of this assertion must be `1`. The value `1` indicates that you can log in to the web client only once using this token.
- **Prn, sub, or upn**: Any of these assertions can be used for the JD Edwards EnterpriseOne user ID.

This is an example of a recommended payload for the JWT:

```
{
 "jti":"caf728cb-44d0-4f4b-bacf-7d588f7c3f1f",
 "prn":"E1USER",
 "iat":1616427984,
 "exp":1616428104,
 "iss":"issuer",
 "at_use_nbr":1
}
```

Note: After the token is validated and a session is established, the browser will navigate to the EnterpriseOne main page. You can also use a shortcut to navigate directly to the required application. The system then removes the JWT from the URL.

Configuring EnterpriseOne Server Trust of the HTML Server

You need to configure the EnterpriseOne Server Trust of the HTML Server before you configure the HTML Server with a certificate.

Access the Work With Node Configuration form.

1. Ensure that a Trusted Node configuration is already created.

   See *Setting Up a Node Configuration*.
2. Use the Security section of the Server Manager configuration to enter the exact Node Name and Node Password configured for the HTML Server.

   Notice that the Node Password is hidden because the environment is configured with a site key that encrypts all passwords in the configuration files. You can use either configuration, with or without site key.
3. Bounce the EnterpriseOne Server and then the HTML Server.

Adding an Existing Certificate to a New Keystore

Use the Java keytool utility to create a keystore to securely encapsulate the certificate.

1. Locate the keytool inside the JDK bin directory.
2. Make sure the certificate file (.cer) is located on the same machine as the JDK.
3. Execute the keytool command as follows, substituting values for alias, file, and keystore.
   ```
   keytool -import -alias <your-alias> -file <your-cer-file> -keystore <your-keystore-name>
   ```
   e.g.
   ```
   keytool -import -alias abcdomain -file "/usr/certs/mycert.cer " -keystore "/usr/certs/mykeystore.p12"
   ```
4. Enter a password for the keystore, make sure to remember this password as it will be used in configuring the HTML Server in Server Manager.
5. You will be prompted to trust the certificate, type Yes and then click **Enter**.
6. The system stores the keystore in the location you indicated with the .p12 extension.
7. To verify that the certificate is in the keystore, use the following keytool utility command. Enter the password when prompted. The system lists the certs in the store.
   ```
   keytool -list -v -keystore ""/usr/certs/mykeystore.p12"
   ```

Configuring HTML Server with a Certificate

There are two separate configuration sections in Server Manager to allow for all certificates in each store to be trusted. Each section allows for one keystore; multiple certificates can be imported into that keystore.

The external section is for configuring certificates for a JWT token generated outside of the JD Edwards system.

The internal section is for configuring certificates for JWT tokens generated by AIS Servers, for communication between the AIS and HTML Servers (for example, notifications and scheduler). By default, the demo certificate is enabled. The demo certificate is always allowed. If you have enabled the demo certificate and included certificates in a keystore, all of them can be used. The demo certificate will be tried first if it is enabled.

> **Note:** Any certificates that you include in the internal keystore much match the certificates configured for each AIS Server associating with the HTML Server (public/private key pair).

Before you start configuring the HTML Server with a certificate, you need to upload the .p12 file to the machine where the HTML Server is deployed.

Access the Server Manager Configuration form.

1. Select the Security configuration for the HTML Server.
2. For the External OAuth JWT Trust Configuration for Authentication, enter the keystore location details, and the password of the keystore.
3. For the AIS Internal JWT Trust Configuration for Authentication, enter the keystore location details, password of the keystore, and select whether to use the demo certificate.
4. Apply the change, synchronize, and bounce the HTML Server.
5. Make sure the site key is enabled, so the password is encrypted and hidden after the sync/bounce.

Configuring EnterpriseOne HTML Server for JSON Web Token (JWT) (Release 9.2.0.5)

This section discusses how to:

- Understand JSON Web Token Authentication.
- Configure EnterpriseOne Server Trust of the HTML Server.
- Add an existing certificate to a new keystore.
- Configure HTML Server with a certificate.

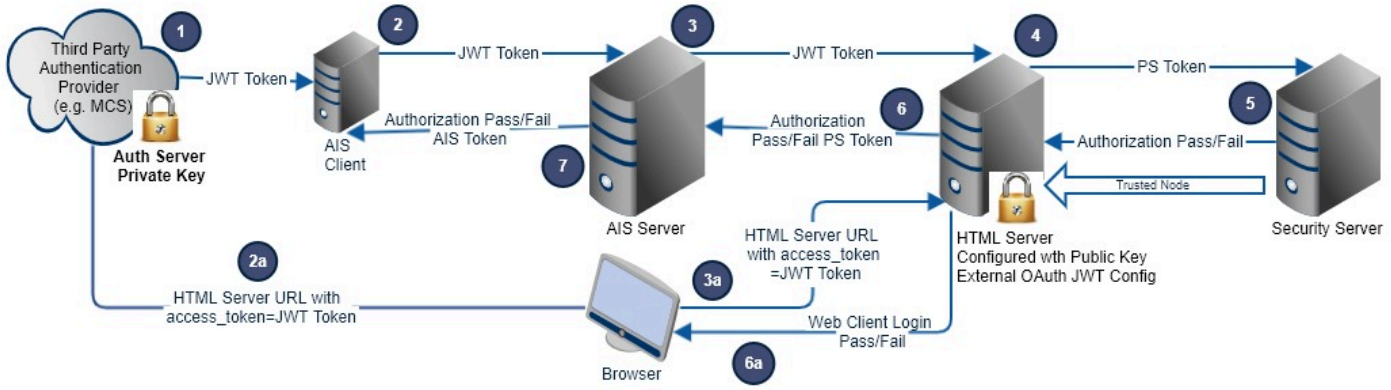
Understanding JSON Web Token Authentication

To provide single sign on access using JD Edwards EnterpriseOne and any JWT producing authority, including Oracle Mobile Cloud Service, you need to configure the EnterpriseOne Server trust of the HTML Server, add an existing certificate to a new keystore, and then configure the HTML Server with a certificate. These configurations allow you to establish a trust relationship between a token provider (such as Mobile Cloud Service) and an EnterpriseOne AIS Server and HTML Server.

For authentication with a JWT, the following must take place:

- The public key certificate used for token generation by the third party must be provided.
- You must store this certificate in a secure Java keystore (.jks) and upload it to the EnterpriseOne HTML Server.
- You must configure the EnterpriseOne HTML Server with the keystore name, keystore password, and certificate alias.
- Principal passed in the JWT must match the EnterpriseOne user ID.
- You must configure the EnterpriseOne HTML Server as a trusted node through a single sign-on trust configuration.

#unique_367/unique_367_Connect_42_CEGCCIEB shows the authentication flow in an environment in which JWT is used for authentication.



The following steps describe the authentication flow:

1. A JWT is generated with the private key and sent in the Bearer header of an AIS token request. (Stateless requests are also supported).
2. The JWT is forwarded to the EnterpriseOne HTML Server by the AIS Server in the Bearer if login is required, and the AIS Server is configured to allow a JWT.
3. The JWT is validated against the public key, the token timeout is validated, and the principal (user) is extracted from the JWT payload. A PS Token is generated for that user and sent for authorization by the Security Server (EnterpriseOne Enterprise Server).
4. The Security Server checks the PS token with SSO node trust, and then an authorization response is returned to the EnterpriseOne HTML Server.
5. The authorization response is returned to the AIS Server. The PS Token is included in the response.
6. The authorization response is returned to the AIS client (third-party). If passed, for a token request the response includes an AIS token.

Configuring EnterpriseOne Server Trust of the HTML Server

You need to configure the EnterpriseOne Server Trust of the HTML Server before you configure the HTML Server with a certificate.

Access the Work With Node Configuration form.

1. Ensure that a Trusted Node configuration is already created.

   See *Setting Up a Node Configuration*.

2. Use the Security section of the Server Manager configuration to enter the exact Node Name and Node Password configured for the HTML Server.

   Notice that the Node Password is hidden because the environment is configured with a site key that encrypts all passwords in the configuration files. You can use either configuration, with or without site key.
3. Bounce the EnterpriseOne Server and then the HTML Server.

Adding an Existing Certificate to a New Keystore

Use the Java keytool utility to create a keystore to securely encapsulate the certificate.

1. Locate the keytool inside the JDK bin directory.
2. Make sure the certificate file (.cer) is located on the same machine as the JDK.
3. Execute the keytool command as follows, substituting values for alias, file, and keystore.

   ```
   keytool -import -alias <your-alias> -file <your-cer-file> -keystore <your-keystore-name>
   ```

   e.g.

   ```
   keytool -import -alias abcdomain -file "/usr/certs/mycert.cer " -keystore "/usr/certs/mykeystore.jks"
   ```
4. Enter a password for the keystore, make sure to remember this password as it will be used in configuring the HTML Server in Server Manager.
5. You will be prompted to trust the certificate, type Yes and then click **Enter**.
6. The system stores the keystore in the location you indicated with the .jks extension.
7. To verify that the certificate is in the keystore, use the following keytool utility command. Enter the password when prompted. The system lists the certs in the store.

   ```
   keytool -list -v -keystore ""/usr/certs/mykeystore.jks"
   ```

Configuring HTML Server with a Certificate

Before you start configuring the HTML Server with a certificate, you need to upload the .jks file to the machine where the HTML Server is deployed.

Access the Server Manager Configuration form.

1. Select the Security configuration for the HTML Server and enter the certificate location details, the password of the keystore, and the alias of the certificate.
2. Apply the change, synchronize, and bounce the HTML Server.
3. Make sure the site key is enabled, so the password is encrypted and hidden after the sync/bounce.

Setting Up a Token Lifetime Configuration Record

A node that has a token lifetime configuration always generates a pair of lifetime configuration records—one for the regular token and one for the extended token. The trusted node configuration depends on the token lifetime configuration. You can add a pair of new token lifetime configuration records for an existing node.

This section discusses how to:

- Add a token lifetime configuration record.
- Delete a token lifetime configuration record.

Adding a Token Lifetime Configuration Record

Access the SSO Environment Configuration Tools form. In JD Edwards Solution Explorer, select System Administration Tools (GH9011), User Management, User Management Advanced and Technical Operations, and then double-click SSO Environment Configuration Tools.

1. Click the **Single Signon Token Lifetime Configuration** link.
2. On the Work With Token Lifetime Configuration form, click **Add**.
3. On the Token Lifetime Configuration Revision form, complete these fields:
   - Regular Token Lifetime
     Specify the expiration time for a regular token. The default value for a node is 720 minutes (12 hours).
   - Extended Token Lifetime
     Specify the expiration time for an extended token. The default value is 4320 minutes (three days). However, the recommended value for this setting is 43,200 minutes (30 days).

Deleting a Token Lifetime Configuration Record

Access the Work With Token Lifetime Configuration form.

> **Note:** If one token lifetime configuration record is deleted, then another token lifetime configuration for the same node and the trusted node configurations that have this node in it will be deleted as well.

On the Work With Token Lifetime Configuration form, select a node and then click the Delete button.

> **Note:** A dialog box appears warning you that if you delete this record, the system will delete the extended and regular token lifetime configuration records and the trusted node configuration records of this node.

Setting Up a Trusted Node Configuration

This section discusses how to:

- Add a trusted node configuration.
- Delete a trusted node configuration.

Adding a Trusted Node Configuration

The nodes that you add to a new trusted node configuration must already be defined and have token lifetime configuration records.

Access the SSO Environment Configuration Tools form. In JD Edwards Solution Explorer, select System Administration Tools (GH9011), User Management, User Management Advanced and Technical Operations, and then double-click SSO Environment Configuration Tools.

1. Click the **Single Signon Trusted Node Configuration** link.
2. On the Work With Trusted Node Configuration form, click Find, select a record, and then click **Add**.
3. On the Trusted Node Configuration Revision form, enter a node in the Node Name field and then click **OK**.

Deleting a Trusted Node Configuration

Access the Work With Trusted Node Configuration form.

Select a record and then click Delete.

Configuring Single Sign-On for a Pre-EnterpriseOne 8.11 Release

EnterpriseOne stores single sign-on node configuration information in new tables (F986180, F986181 and F986182). These tables are not available in pre-8.11 releases (such as release 8.94). However, you can still configure single sign-on for the pre-release through single sign-on node settings in the jde.ini file.

This section discusses how to:

- Modify jde.ini file node settings for single sign-on.
- Work with sample jde.ini node settings for single sign-on.

Modifying jde.ini file Node Settings for Single Sign-On

EnterpriseOne comes with standard default settings for single sign-on. If you do not want to accept the default settings, you can overwrite the default single sign-on node settings by configuring the jde.ini file.

See *Understanding the Default Settings for the Single Sign-On Node Configuration*.

Access the jde.ini file to modify the single sign-on node settings.

In the [TRUSTED NODE] section of the jde.ini file, add the appropriate values to these settings:

Setting	Description
numTrustedNodes	Enter the number of trusted nodes.
RegularLifeTime	Enter the expiration time (in minutes) for a regular token.
ExtendedLifeTime	Enter the expiration time (in minutes) for an extended token.
NodeName	Enter the logical name for the first node.

Setting	Description
MachineName	Enter the number of trusted nodes.
NodePassword	Enter the password for the first node.
NodeName1	Enter the logical name for the second node.
MachineName1	Enter the physical machine name for the second node.
NodePassword1	Enter the password for the second node.

Working with Sample jde.ini Node Settings for Single Sign-On

This section contains examples of node settings in the jde.ini file for single sign-on configurations:

Example 1:

A system administrator wants to install the EnterpriseOne system on three machines: SUN1, IBM1 and HP1. He wants all three machines to trust each other, and no other machines will be trusted. In this case, the administrator can configure the jde.ini as follows and deploy it on SUN1, IBM1, and HP1:

```
[TRUSTED NODE]
numTrustedNodes=3
```

For Sun:

```
NodeName=NodeSUN1
MachineName=SUN1
NodePassword=NodePwd
```

For IBM:

```
NodeName1=NodeIBM1
MachineName1=IBM1
NodePassword1=IBM1Pwd
```

For HP:

```
NodeName2=NodeHP1
MachineName2=HP1
NodePassword2=HP1Pwd
```

Example 2:

A system administrator wants all EnterpriseOne servers in the network to trust each other. Moreover, he wants to change the default node configuration as follows:

- Change the node password to NewPwd.

- Change the regular token lifetime to 30 minutes instead of 12 hours.
- Change the extended token lifetime to 60 minutes instead of 30 days.

In this case, the administrator can configure the jde.ini as follows and deploy it to all the enterprise servers in the network:

```
[TRUSTED NODE]
numTrustedNodes=1
RegularLifeTime=30
ExtendedLifeTime=60
NodeName=_GLOBALNODE (The node name must be _GLOBALNODE)
MachineName=_GLOBALNODE (The machine name must be _GLOBALNODE)
NodePassword=NewPwd
```

Configuring Single Sign-On Without a Security Server

When there is no security kernel available in the system, a user can directly sign in to the EnterpriseOne Windows client without using the security server. To sign in to EnterpriseOne without a security server, you must:

- Set SecurityServer=<blank> in the [SECURITY] section of the client jde.ini file.
- Sign on to EnterpriseOne using the system (database) user ID and password.

In this case, the EnterpriseOne Windows client generates an authenticate token locally. This token is referred to as a local token. A local token is very similar to a regular token except that it has a fixed node name (_LOCALNODE) and contains the system user name and password. A local token can only be accepted by a local fat client or an enterprise server without a security server, for example SecurityServer=<blank> in the server jde.ini.

> **Note:** If you sign in to EnterpriseOne without a security server, you can only run the business functions and UBEs that are mapped to either the local machine or the enterprise server without a security server.

When a local token is used, the default value for regular token lifetime is 12 hours and the default value for extended token lifetime is 30 days. You can override these default values for the local token using the SSO Environment Configuration Tools application or by modifying the appropriate settings in the jde.ini file of the Windows client, deployment server, and enterprise server.

These are sample jde.ini node settings to override _LOCALNODE for the local token:

```
[TRUSTED NODE]
numTrustedNodes=1
RegularLifeTime=4320
ExtendedLifeTime=43200
NodeName=_LOCALNODE
MachineName=_LOCALNODE
```

> **Note:** You cannot override the node password for _LOCALNODE in the jde.ini file; you must use the SSO Environment Configuration Tools application to do this.

16 Setting Up JD Edwards EnterpriseOne Single Sign-On Through Oracle Access Management 11g Release 2

Understanding JD Edwards EnterpriseOne Single Sign-On Through Oracle Access Management

Oracle Access Management (OAM) provides single sign-on functionality for Oracle applications, including JD Edwards EnterpriseOne. It provides a secure internet infrastructure for identity management for EnterpriseOne applications and processes. This infrastructure provides:

- Identity and access management across EnterpriseOne applications, enterprise resources, and other domains.
- Foundation for managing the identities of customers, partners, and employees across internet applications. These user identities are protected by security policies for web interaction.

Integration with OAM provides EnterpriseOne implementations with these features:

- OAM authentication, authorization, and auditing services for EnterpriseOne applications.
- OAM single sign-on for EnterpriseOne applications and other OAM-protected resources in a single domain or across domains.

  > **Note:** EnterpriseOne single sign-on through OAM is supported only by the EnterpriseOne web client, not Collaborative Portal.

- OAM authentication schemes that provide single sign-on for EnterpriseOne applications:
  - Basic Over LDAP (Lightweight Directory Access Protocol): Users enter a user name and password in a window supplied by the web server.

    This method can be redirected to Secure Socket Layer (SSL).
  - Form: Similar to the basic challenge method, users enter information in a custom HTML form.

    You choose the information that users must provide in the form.
  - X509 Certificates: X.509 digital certificates over SSL.

    A user's browser must supply a certificate.
  - Integrated Windows Authentication (IWA): Users will not notice a difference between an OAM authentication and IWA when they log on to the desktop, open a browser, request an OAM-protected web resource, and complete single sign-on.
  - Microsoft .NET Passport: NET Passport is a component of the Microsoft .NET Framework. The .NET plug-in is a web-based authentication service that provides single sign-on for Microsoft-protected web resources.
  - Custom: You can use other forms of authentication through the OAM Authentication Plug-in API.
- Session timeout: OAM enables you to set the length of time that a user session is valid.

- Ability to use Oracle Identity Manager for identity management. Oracle Identity Manager provides identity management features such as portal inserts, delegated administration, workflows, and self-registration EnterpriseOne applications.

  You can determine how much access to provide to users upon self-registration. Oracle Identity Manager workflows enable a self-registration request to be routed to appropriate personnel before access is granted. OAM also provides self-service, enabling users to update their own identity profiles.

Note:

- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite* and the Oracle Identity Manager documentation.

JD Edwards EnterpriseOne Integration Architecture

EnterpriseOne has a configurable authentication mechanism that allows it to authenticate a user against:

- Native tables (through a security kernel)
- Lightweight Directory Access Protocol (LDAP)
- Custom plug-ins, including the ability to read HTTP headers

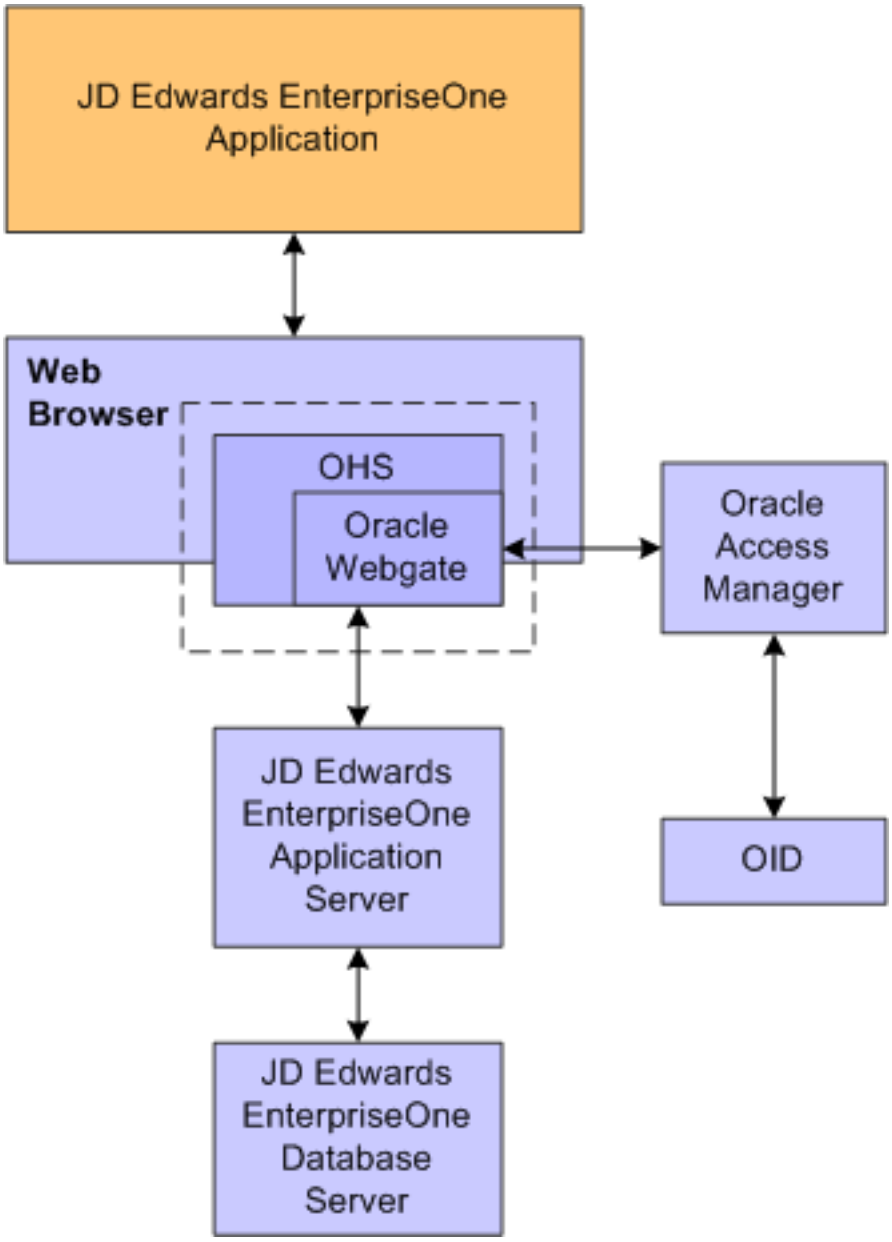
EnterpriseOne single sign-on through OAM involves:

- Protection through a WebGate, which is a plug-in that intercepts web resource (HTTP) requests and forwards them to the Access Server for authentication and authorization.
- Populating a header variable with an attribute value that is stored in the LDAP directory used by OAM.
- Configuring EnterpriseOne to invoke the OAM authentication process, overriding the default authentication mechanism.

Single Sign-On Architecture

Single sign-on with OAM requires an EnterpriseOne HTML Server configuration with an application server, such as Oracle WebLogic Server 10g, that contains a J2EE container, which is required for the Java servlets and Java code to run. In addition, WebGate must be installed on an Oracle HTTP Server, and it must be configured to protect the EnterpriseOne URLs that are used to access the HTML Server.

This illustration shows the integration environment and process flow:



The following steps describe the single sign-on process:

1. A user attempts to access an EnterpriseOne program by entering a URL to the EnterpriseOne web client in a web browser.
2. A WebGate deployed on the EnterpriseOne HTTP Server intercepts the request.
3. The WebGate checks OAM to determine whether the resource (EnterpriseOne URL) is protected.
4. If a valid session does not exist and the resource is protected, WebGate prompts the user for credentials through the OAM login page.
5. After the user enters the single sign-on user ID and password on the OAM login page, the WebGate captures the user credentials and sends them to OAM for authentication.
6. OAM compares the user credentials against the Oracle Internet Directory (OID).

    a. If the user's single sign-on credentials are not in OID, OAM notifies WebGate and the user is denied access to EnterpriseOne.

   b. If OAM finds the user's single sign-on credentials in OID, OAM authenticates the credentials.
7. If the credentials are validated, the user gains access to the EnterpriseOne web client.
8. If a valid session already exists and the user is authorized to access the resource, WebGate redirects the user to the requested EnterpriseOne resource.

Supported Versions and Platforms

For supported versions and platforms for the integration of OAM with JD Edwards EnterpriseOne Tools, JD Edwards EnterpriseOne Applications, and JD Edwards EnterpriseOne HTML Server see the Certifications tab on My Oracle Support:

https://support.oracle.com/epmos/faces/CertifyHome?_adf.ctrl-state=78o46rofa_43&_afrLoop=34652538504327

Prerequisites

In addition to single sign-on configuration instructions, this chapter contains instructions on how to install Oracle Identity and Access Management 11gR2, which requires the following prerequisites:

- Create the OAM schemas through Oracle Repository Utility (RCU).

  Note: The Oracle Repository Utility version **must** match the product that you are installing.

- Install Oracle WebLogic Server.
- Obtain the JDK 1.7 update 80 or later and the Oracle Identity and Access Management installation images from Oracle Software Delivery Cloud.

Installing Oracle Identity and Access Management

This section provides basic installation instructions to support a single sign-on configuration for EnterpriseOne. If your configuration requires supporting additional applications, see the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* .

To install Oracle Identity and Access Management:

1. Launch the Oracle Identity and Access Management run Installer (or setup.exe).
2. On the Welcome screen, click **Next**.
3. Select the **Install Software Updates** option.

   The installer performs a prerequisites check.
4. Specify the Oracle Middleware Home and accept the default Oracle Home Directory name.
5. Review the Installation Summary and click **Install**.
6. Click **Finish** when the installation is complete.

Setting Up OAM to Support an EnterpriseOne Single Sign-on Configuration

After installing Oracle Identity and Access Management, perform the following tasks:

- *Creating a New OAM Domain*
- *Configuring the Database Security Store for an Oracle Identity and Access Management Domain*
- *Registering the WebGate Agent for JD Edwards EnterpriseOne HTML Server*
- *Creating Additional Authentication Policies and Resource*
- *Configuring the EnterpriseOne SSO Parameter*
- *Copying the WebGate Artifact to the Oracle HTTP Server*
- *Configuring Oracle HTTP Server for the EnterpriseOne HTML Server*

Creating a New OAM Domain

To create a new OAM domain:

1. Launch config.sh (.cmd) from the `MW_Home/Oracle_IDM1/common/bin` directory.
2. Select the required Oracle Access Manager option. Other required products will be selected automatically.
3. Enter a domain name.
4. Enter the Administrator user name and password.
5. Select **Production Mode** and verify the JDK location.
6. On Configure JDBC Component Schema, enter the JDBC component schema information. You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port.

   Select each component schema one at a time because the schema owners are different.

   The schemas should have already been created using the Oracle Repository Utility (RCU) as described in the *Prerequisites* section in this chapter.
7. Click **Next** to verify the connections.
8. Select the **Administration Server** and then select the **Managed Servers**, **Clusters**, and **Machines** options.

   You can accept the default values for the Administration Server and Port.
9. Enter or accept the default Managed Server name, `oam_server1`.
10. Click **Next** to skip the Cluster configuration.
11. Click **Add** to configure the Machine information.
12. Assign the servers from the left pane after the machine is created.
13. Review the Configuration Summary and click **Create**.
14. Click **Finish** when complete.

    Before you start the WebLogic Administration Console, complete the steps in the remaining tasks in this section.

Configuring the Database Security Store for an Oracle Identity and Access Management Domain

You must run the configureSecurityStore.py script to configure the Database Security Store. This is the only security store type supported by Oracle Identity and Access Management 11g Release 2.

There are two options to configure the Database Security Store:

- **-m create**
- **-m join**

The instructions in this chapter use the create option because the join option is for additional domains to use the same Database Security Store already created.

To configure a domain to use a database security store using the -m create option, you must run the configureSecuirytStore.py script as follows depending on your platform:

- **On Windows**:

  ```
  MW_home\oracle_common\common\bin\wlst.cmd <IAM_Home>\common\tools\configureSecurityStore.py -d
  <domaindir> -c IAM -p <opss_schema_pwd> -m create
  ```

- **On UNIX**:

  ```
  MW_home/oracle_common/common/bin/wlst.sh <IAM_Home>/common/tools/configureSecurityStore.py -d
  <domaindir> -c IAM -p <opss_schema_pwd> -m create
  ```

Note: For both platforms, the -c option must be specified as IAM.

The following is sample output from the script:

```
Using default context in /u01/Oracle/Middleware/user_projects/domains/IDM_domain/config/
fmwconfig/jps-config-migration.xml file for credential store.
Credential store location : jdbc:oracle:thin:@myserver.com:1521/orcl
Credential with map Oracle-IAM-Security-Store-Diagnostics key Test-Cred stored
 successfully!
 Credential for map Oracle-IAM-Security-Store-Diagnostics and key Test-Cred is:
               GenericCredential
Info: diagnostic credential created in the credential store.
Info:  Create operation has completed successfully.
```

At this point, you can start the Domain Administration Server and the Managed Server.

Registering the WebGate Agent for JD Edwards EnterpriseOne HTML Server

1. Sign in to Oracle Access Management Console.
2. Open the Oracle Access Management Console, for example, **http://oamserver:oamport/oamconsole**
3. Enter the Admin user name and password.
4. On the Launch Pad, select the **SSO Agent Registration** from the Quick Start Wizards section.

5. Select your WebGate, for example 11g WebGate, and click **Next**.
6. In the Configuration section, enter a name and description for the WebGate.
7. In the Security Option area, select the **Open** option, and then click **Finish**.

   If successful, the system displays a confirmation message and shows the location in which the artifacts are stored. Entries are also created for the new WebGate under the Host Identifiers and Application Domains nodes.
8. To see the entry under Host Identifiers, on the Launch Pad, open the **Host Identifiers** from the Access Manager section, and then click **Search**.

   OAM displays a list of host identifiers.
9. To see the entry under Application Domains, on the Launch Pad, open the Application Domains from the Access Manager section, and then click Search.

   OAM displays a list of application domains.

Creating Additional Authentication Policies and Resource

1. Open the Oracle Access Management Console.
2. Select **Application Domains** from the Access Manager section.
3. Click **Search** and select your domain name, and then click **Edit**.
4. Select the **Authentication Policies** tab.
5. Click **Create Authentication Policy** button.
6. Create the following policies with your Authentication Scheme.
   - E1Menu Policy
   - ParameterizedURL Policy
   - ShortcutLauncher Policy
7. Click the **Resources** tab to create HTTP Type Resources for these policies.
8. Create the following policies for the Protected Resource Policy:
   - `/`
   - `/.../*`
   - `/jde`
9. Create the following resource for the E1Menu Policy:

   ```
   /jde/E1Menu.maf
   ```
10. Create the following resource for the Parameterized URL Policy:

    ```
    /jde/HostedE1Servlet
    ```

11. Create the following resources for the ShortcutLauncherPolicy:

    - **`/jde/ShortcutLauncher`**
    - **`/jde/servlet/com.jdedwards.runtime.shortcut.ShortcutLauncher`**

    The output should be similar to the following example:

Actions ▾ View ▾ | Create | Duplicate | Edit | Delete | Detach

Row	Resource Type	Host Identifier	Resource URL	Query String	Authentication Policy	Authorization Policy
1	HTTP	WNAssoEnterpr...	/jde/servlet/com.jdedwar...		ShortcutLauncherPolicy	Protected Resource Policy
2	HTTP	WNAssoEnterpr...	/jde/ShortcutLauncher		ShortcutLauncherPolicy	Protected Resource Policy
3	HTTP	WNAssoEnterpr...	/jde/HostedE1Servlet		ParameterizedURL Policy	Protected Resource Policy
4	HTTP	WNAssoEnterpr...	/jde/E1Menu.maf		E1Menu Policy	Protected Resource Policy
5	HTTP	WNAssoEnterpr...	/jde		Protected Resource Policy	Protected Resource Policy
6	HTTP	WNAssoEnterpr...	/.../*		Protected Resource Policy	Protected Resource Policy
7	HTTP	WNAssoEnterpr...	/*		Protected Resource Policy	Protected Resource Policy
8	HTTP	WNAssoEnterpr...	/**		Protected Resource Policy	Protected Resource Policy

Columns Hidden 2

12. Enter the EnterpriseOne URL to the Success URL field in the Protected Resource Policy.

Create Authentication Policy Authentication Policy — Apply

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

* Name: Proctected Resource Policy

Description: Policy set during domain creation. Add resources to this policy to protect them.

Success URL: http://myserver:7777/jde/E1Menu.maf

Failure URL:

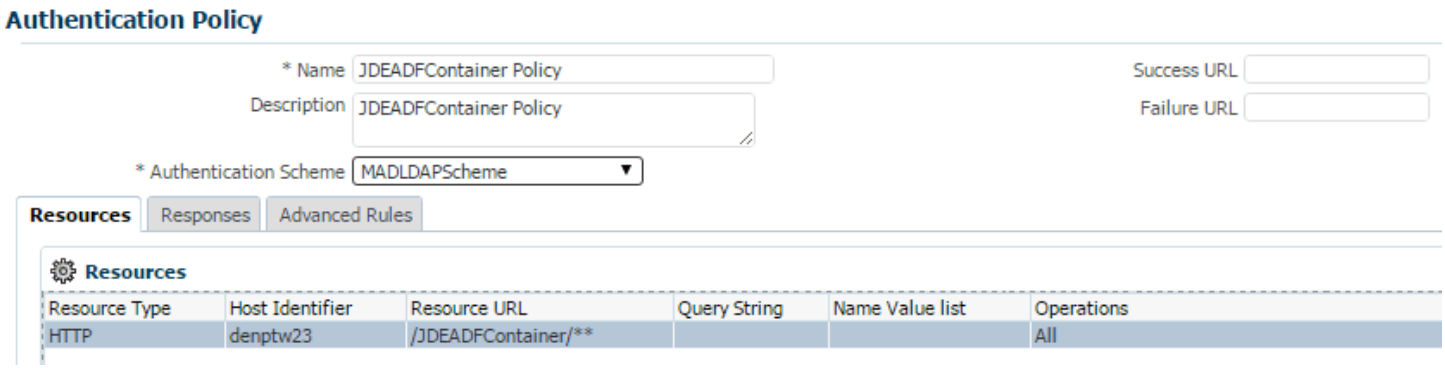
13. Create another HTTP Type Resource for the logout notification that will not be added to any Authentication or Authorization Policy:

    - **`/jde/NotificationController.mafService`**

    Select *POST* for the Operation of this resource.

    Select *Excluded* for the Protection Level of this resource.

14. This step applies only to Oracle Access Management (OAM) for Application Development Framework (ADF) Container.

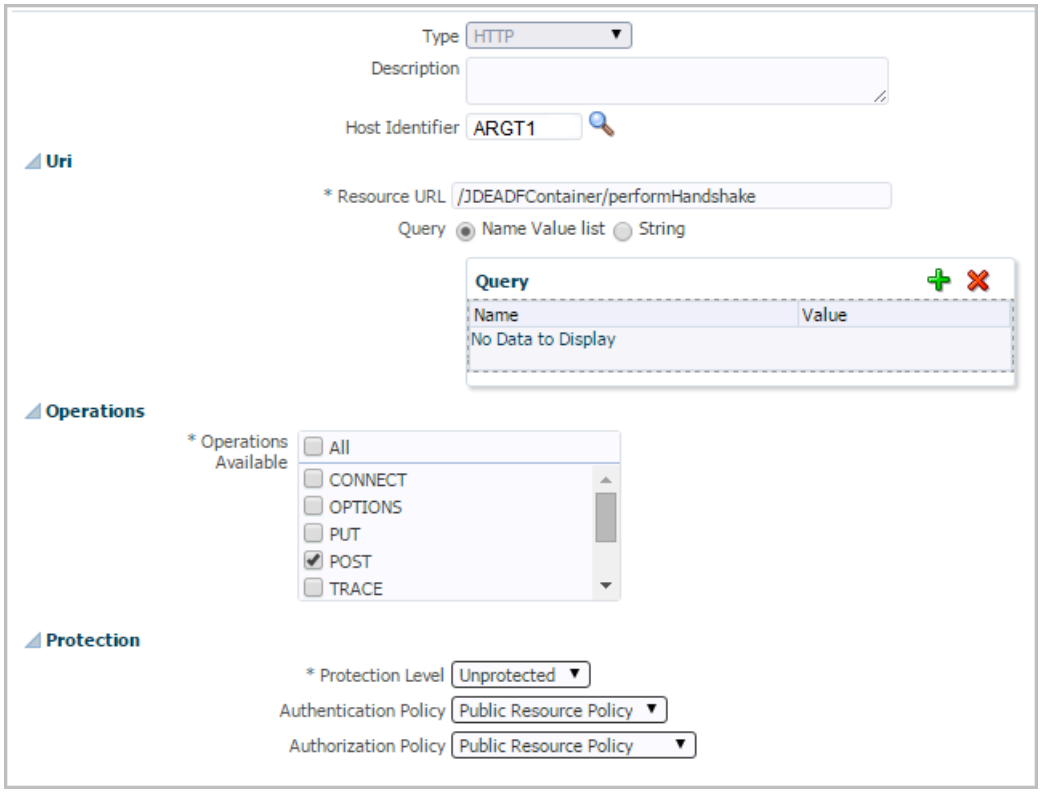


Create the following policy for Protected Resource Policy:

- **`/JDEADFContainer/**`**

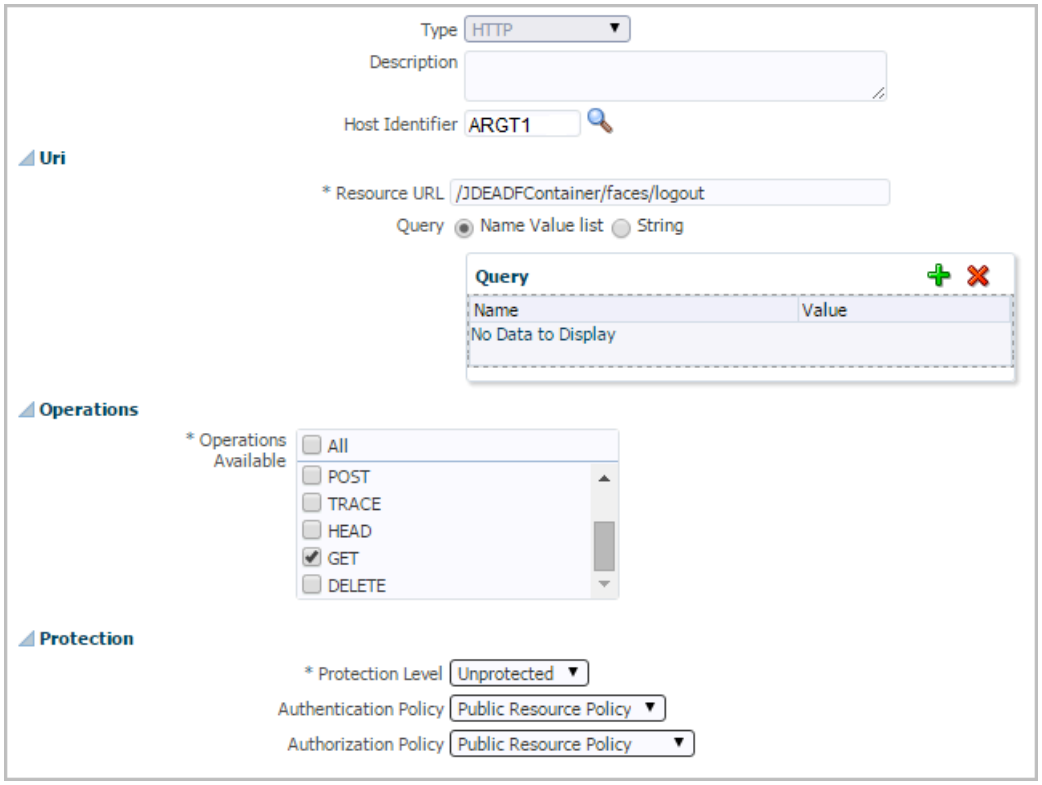
Create the following policies for the Public Resource Policy:

- **`/JDEADFContainer/performHandshake`**



Only *POST* operation should be selected for this resource.

- **`/JDEADFContainer/faces/logout`**



Only *GET* operation should be selected for this resource.

For information about the configuration settings for JAS, ADF, AIS Cookies and ADF settings using Server Manager, see "Configuring Oracle Access Management (OAM) for ADF Container" in the *JD Edwards EnterpriseOne Tools Developer's Guide for EnterpriseOne Application Development Framework (ADF) Applications*.

Configuring the EnterpriseOne SSO Parameter

1. Open the Oracle Access Management Console.
2. Select **Application Domains** from the Access Manager section.
3. Click **Search** and select your domain name, and then click **Edit**.
4. Select the **Authorization Policies** tab.
5. Select the **Protected Resource Policy**.
6. Click the **Responses** tab and click the plus (**+**) sign.
7. In the Add Response area, complete the following fields:
   - **Type**. From the drop-down menu, select Header.
   - **Name**. Enter JDE_SSO_UID in this field.
   - **Value**. Enter $user.userid in this field.
8. Click the **Add** button.
9. Click **Search** and open E1OHS12cWebgate.
10. Select the **Authorization Policies** tab.
11. Select the **Protected Resource Policy**.

12. Click the **Responses** tab and click the plus (**+**) sign.
13. In the Add Response area, complete the following fields:
    - **Type**. From the drop-down menu, select Header.
    - **Name**. Enter JDE_SSO_TOKEN in this field.
    - **Value**. Enter ${session.id} in this field.

Copying the WebGate Artifact to the Oracle HTTP Server

After registering the SSO agent, verify the cwallet.sso and OBAccessClient.xml files have been created in the following directory:

```
<MW_Home>/user_projects/domain/IDMDomain/output/<SSO_Agent_Name>
```

Copy the cwallet.sso and OBAccessClient.xml files to the WebTier home on the Oracle WebTier (OHS) Server. For example:

```
<MW_Home>/Oracle_WT1/instances/instance1/config/OHS/ohs1/webgate/config
```

Configuring Oracle HTTP Server for the EnterpriseOne HTML Server

After you install and configure the Oracle HTTP Server and Oracle HTTP WebGate, you will need to configure the mod_wl_ohs.conf file.

To configure the mod_wl_ohs.conf file:

1. Navigate to the mod_wl_ohs.conf file located at:

   ```
   2. <MW_Home>/user_projects/domain/<oamdomain>/config/fmwconfig/components/OHS/
   instances/<ohs_instance_name>/
   ```
2. Edit the mod_wl_ohs.conf file.
   a. Add a Virtual Host section.

      ```
      NameVirtualHost *:7777
      <VirtualHost *:7777>
        <Location /jde>   <--EnterpriseOne Context
          SetHandler weblogic-handler
          WebLogicHost myserver.com
          WebLogicPort 9003  <-- EnterpriseOne Port
        </Location>
      </VirtualHost>
      ```
   b. If you prefer to use the single signon for the WebLogic console, then include a <Location /console> section.

      ```
      <Location /console>  <--WebLogic Console Configuration (optional)
          SetHandler weblogic-handler
          WebLogicHost myserver.com
          WebLogicPort 9001
      </Location>
      ```

c. This step applies only to Oracle Access Management (OAM) for Application Development Framework (ADF) Container.

   If a virtual host section already exists for EnterpriseOne, you only need to add the Location section under the same Virtual Host section.

   For JAS, add a Virtual Host section for ADF container:

```
NameVirtualHost *:7778
<VirtualHost *:7778>
  <Location /JDEADFContainer>   <--ADF Container
    SetHandler weblogic-handler
    WebLogicHost myserver.com
    WebLogicPort 9104  <-- ADF Container Port
  </Location>
</VirtualHost>
```

   For information about the configuration settings for JAS, ADF, AIS Cookies, and ADF settings using Server Manager, see "Configuring Oracle Access Management (OAM) for ADF Container" in the *JD Edwards EnterpriseOne Tools Developer's Guide for EnterpriseOne Application Development Framework (ADF) Applications*.

Note: The HTTP port number (for example: 7777) will be the SSO port.

3. Restart the HTTP server.
   a. Change the directory to Webtier's instance. For example, **`<MW_Home>/Oracle_WT1/instances/<Instance_Name>/bin`**
   b. Run **`./opmnctl stopall`**
   c. Run **`./opmnctl startall`**

Setting Up EnterpriseOne for Single Sign-On Integration with OAM

To set up the EnterpriseOne HTML Server for single sign-on integration with OAM through EnterpriseOne Server Manager:

1. Open Server Manager from a web browser.
2. Select your EnterpriseOne HTML Server instance.
3. In the Configuration section, select **Security Settings**.
4. In the Security Server Configuration section, select the **Enable Oracle Access Manager** option.
5. Enter the Oracle Access Manager (OAM) sign-off URL. This sign-off URL should include the OAM server URL, for example:

   `http://OAMServer:OHSport/oam/server/logout.html?end_url=http://OAMserver:OHSport/jde/index.jsp`

   Also, you can find the sign-off URL in the SSO agent that you set up in the OAM Console, as described in *Registering the WebGate Agent for JD Edwards EnterpriseOne HTML Server*. In the OAM Console, select **SSO Agents** and then search for and open the SSO agent. The sign-off URL is in the Logout Redirect URL field.
6. Click **Apply**.
7. At the prompt, click the **Synchronize** button to synchronize the changes in all .ini files.

8. Stop and restart the EnterpriseOne HTML Server.

To set up the EnterpriseOne ADF Server for single sign-on integration with OAM through EnterpriseOne Server Manager:

1. Open Server Manager from a web browser.
2. Select your EnterpriseOne ADF Server instance.
3. In the Configuration section, select **Security Settings.**
4. Add OHS host and port in the HTML server whitelist field.

   `http://OAMServer:OHSport`
5. Click **Apply.**
6. At the prompt, click the **Synchronize** button to synchronize the changes in all .ini. files.
7. Stop and restart the EnterpriseOne ADF Server.

Note: To integrate Content and Experience Cloud with SSO enabled JD Edwards EntepriseOne HTML Server, you must enable SSO for Content and Experience Cloud with the same on-premise OAM. See *Configuring Federation SSO in Content and Experience Cloud (Release 9.2.2 Update)* for more information.

Setting Up OAM SSO Validation for JD Edwards EnterpriseOne (9.2.6)

To set up the SSO token in OAM for JD Edwards EnterpriseOne:

1. Open the Oracle Access Management Console.
2. Select **Application Domains** from the Access Manager section.
3. Click **Search** and select your domain name, and then click **Edit**.
4. Select the **Authorization Policies** tab.
5. Select the **Protected Resource Policy**.
6. Click the **Responses** tab and click the plus (**+**) sign.
7. In the Add Response area, complete the following fields:
   - **Type**. From the drop-down menu, select Header.
   - **Name**. Enter JDE_SSO_TOKEN in this field.
   - **Value**. Enter ${session.id} in this field.
8. Click the **Add** button.
9. Access the Server Manager for JD Edwards EnterpriseOne.
10. Select the HTML Web Server that you wish to set up the SSO Validation.
11. Navigate → Configuration → Security → Security Server Configuration
12. For OAM 12c only, you must complete the following fields:
    - *SSO Sign-on Validator Path*

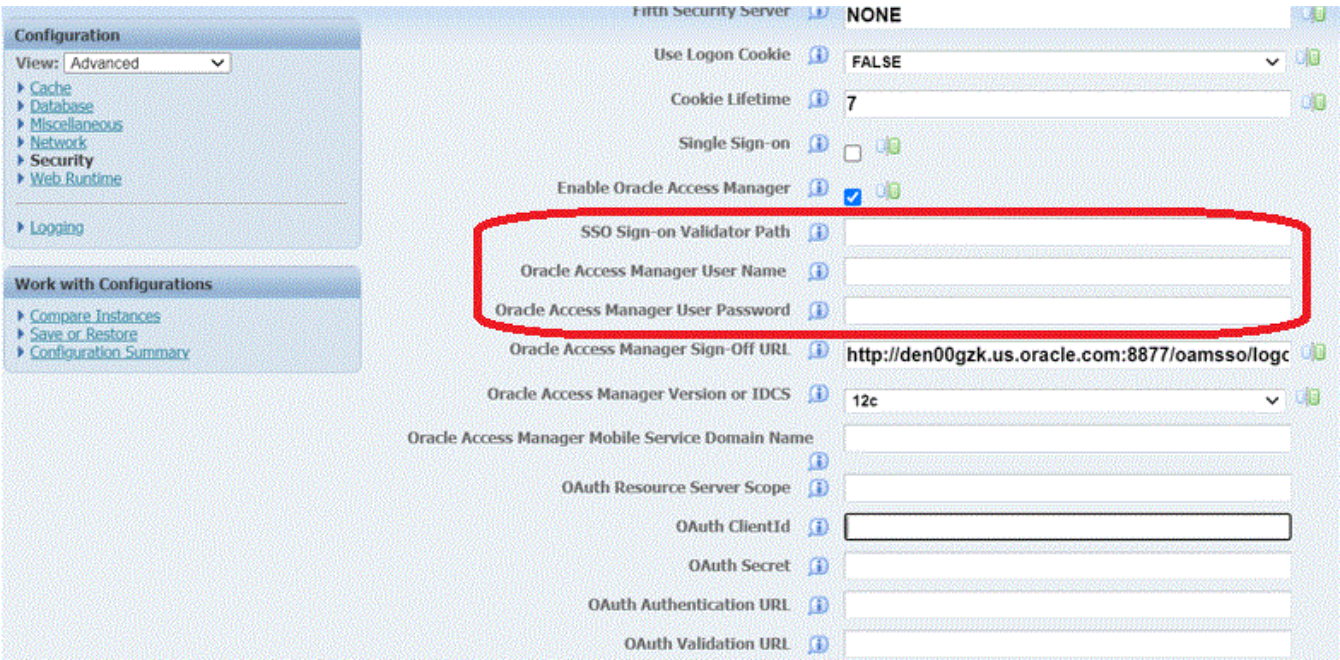
      Enter a value using this syntax:

      http://<machine_name>:<port>/oam/services/rest/access/api/v1/session/
    - *Oracle Access Manager User Name*

      Enter value for a user name.

- *Oracle Access Manager User Password*

  Enter value for the password for the user name you specified for the Oracle Access Manager user name.



Configuring SSO Support for EnterpriseOne AIS Server Clients

In an EnterpriseOne single sign-on setup through Oracle Access Manager (OAM), an additional configuration is required to support single sign-on with applications that run on the AIS Server, which include EnterpriseOne mobile enterprise applications. This setup is also required to support E-Signatures in an EnterpriseOne SSO configuration.

To configure single sign-on support with OAM for AIS clients:

- *Enable the "Mobile and Social" Service in OAM*
- *Configure the Identity Store - Directory Service*
- *Configure the Mobile Service*

- *Configure OAM Mobile Settings for the Enterprise Server in Server Manager*

Enable the "Mobile and Social" Service in OAM

1. In OAM, navigate to Configuration, Available Services.
2. If not enabled, click the **Mobile and Social** service to enable it.

Configure the Identity Store - Directory Service

Create a new Identity Directory Service (IDS) Profile. This IDS Profile requires the same LDAP details used to create your Identity Store for SSO, including Oracle Identity Manager (or other supported LDAP directory) credentials, domain names, and so forth. See *Creating Identity Store in OAM Console* for more information.

The new IDS Profile creates both the IDS Profile and IDS Repository.

To create a new IDS profile:

1. Open the Oracle Access Management (OAM) console.
2. Click **Configuration** and then click **User Identity Stores**.
3. In the IDS Profiles section, click **Create**.
4. Enter the LDAP connection information, modifying the object classes to filter users based on the groups you want to use.
   You have to have at least one object class filter for users and groups.
5. Click **Create**.

Configure the Mobile Service

You can configure the default provider and service or create your own. These steps describe how to configure the default provider.

1. Navigate to **Mobile Security**, **Mobile and Social Services**.
2. In the Service Providers section, select **JWTAuthentication** and click **Edit**.
3. Edit the Identity Directory Service Name to point to the new IDS Profile you just created.
4. Click the **Mobile Services** tab.
5. In the Service Profiles section, select the **JWTAuthentication** row and click **Edit**.
6. Edit the profile, taking note of the URLs listed for User Token and Access Token. You will use these later to configure the OAM settings for the EnterpriseOne Enterprise Server.

Configure OAM Mobile Settings for the Enterprise Server in Server Manager

1. In Server Manager, access the Security Server Configuration settings for the HTML Server.
2. Make sure that the **Enable Oracle Access Manager** check box is selected.
3. Select the Oracle Access Manager Version 11g.
4. Complete the following fields:
   - **Oracle Access Manager Mobile Service Domain Name**. Use Default, leave blank, or if you set up a specific domain for mobile in OAM, enter the domain name here.

- **Oracle Access Manager Mobile Authentication URL**. Enter the URL for the JWT Authentication Service from OAM. This is the URL listed next to the "User Token" setting in OAM.
- **Oracle Access Manager Mobile Tokens URL**. Enter the URL for the JWT Tokens Service from OAM. This is the URL listed next to the "Access Token" setting in OAM.

The Oracle Access Manager Sign-Off URL setting is only for EnterpriseOne web client applications. You can ignore it for this configuration.

5. Complete the configuration by performing the steps in the following sections, after which, users can use their single sign-on username and password to sign on to EnterpriseOne mobile applications.

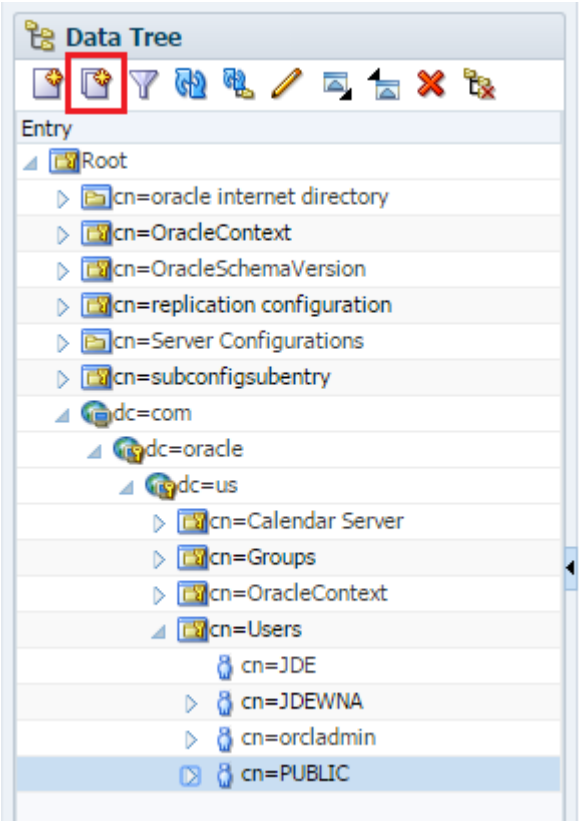
Adding JD Edwards EnterpriseOne HTML Server User to the OID

Oracle Directory Services Manager (ODSM) is required to add a valid JD Edwards EnterpriseOne web client user to Oracle Internet Directory (OID). Complete the following steps to add a user to OID:

1. Enter the ODSM URL in a browser, for example: http://<ServerName>:7005/odsm/faces/odsm.jspx
2. Click **Create A New Connection** from the Connect to a directory menu.
3. Enter a name for the connection in the Name field.
4. Enter a name for the server in the Server field.
5. Enter the ODSM port number in the Port field.
6. Enter the user name in the User Name field. The default value, which should not be changed, is cn=orcladmin.
7. Enter the password.
8. Select a page from the Start Page list that will be displayed when a user connects to this connection.
9. Click **Connect**.
10. Use the connection created in the previous step to connect to the OID.
11. Click the **Data Browser** tab.
12. Expand the dc=com, dc=oracle, dc=us, cn=Users nodes.

13. Click **Create a new entry like this one** to use the properties of an existing user for creating a new user.

    This option uses the values of the existing user to minimize the effort in providing information while creating a new user.



14. In the Entry Properties section in the New Entry dialog box, click Next.
15. In the Mandatory Properties section, specify the JD Edwards username in the ***cn** and the ***sn** fields.

    The value specified in both the fields must be same.
16. Select an option from the Relative Distinguished Name list and click Next.
17. In the Optional Properties section, complete the following fields:
    - description: Specify a description.
    - givenName: Specify the JD Edwards user name specified in the *cn and the *sn.
    - mail: Specify the JD Edwards user name specified in the *cn and the *sn.
    - orclActiveStartDate: Specify the date when the user will be activated.
    - orclIsEnabled: Specify whether the user account is enabled or disabled.
    - uid: Specify the JD Edwards user name specified in the *cn and the *sn.
    - userPassword: Specify the password that will be used to log in to the OAM console.
18. Click **Next**.
19. Expand the cn=Groups node.
20. Click the group that you want to add the user to.
21. Click the plus (**+**) sign above the Members section.
22. Click the entry button to open the Select Distinguished Name (DN) Path dialog box.

23. Expand the dc=com, dc=oracle, dc=us, cn=Users nodes.
24. Select the user you want to add to the group and click **OK**.

Creating Identity Store in OAM Console

1. Open the Oracle Access Management (OAM) console.
2. Click **Configuration**.
3. Click **User Identity Stores** and click **Create**.

   Note: The default port of OID specified in the Location and Credentials section is 3060.

4. Click the **Test Connection** button to test the connection.
5. Set the newly created identity store as default store for OID.
6. Restart the OAM and HTTP server.

Testing the Single Sign-On Configuration

Complete the following steps to test the single sign-on configuration:

1. In a web browser, enter the following URL to access the EnterpriseOne web client:

   `http://yourhost:yourssoport/jde/E1Menu.maf`

   The system displays the OAM 11g login page.
2. On the login page, enter the LDAP user name and password. The LDAP user should also be a valid EnterpriseOne user.

   If the credentials are validated, the system grants access to the EnterpriseOne web client. You have successfully configured single sign-on.

Configuring Federation SSO in Content and Experience Cloud (Release 9.2.2 - Release 9.2.8)

Complete the following steps to configure single sign-on to link a tenant account of Content and Experience Cloud and the on-premise Identity Provider (IdP):

1. Add the Content and Experience Cloud user to the Oracle Internet Directory (OID).

   Note: You must use the email address of the JD Edwards EnterpriseOne user as the user name for creating the Content and Experience Cloud user.

2. Download the on-premise Oracle Access Manager (OAM) IdP SAML 2.0 metadata:
   a. Type the Identity Provider URL in a browser.
   b. Log in using your OAM credentials.
   c. Save the IdP SAML 2.0 metadata file on your computer.

Adding the On-Premise Identity Provider as a Partner in Content and Experience Cloud

1. Log in to the Content and Experience Cloud Dashboard.
2. Click **Users**.
3. Click the **SSO Configuration** tab, and then click **Edit** for the Configure SSO.
4. In the Edit Single Sign-On Configuration dialog box, select the **Import identity provider metadata** option, and then Click **Choose File**.
5. On the Browse window, select the IdP SAML 2.0 metadata file you recently saved on your computer, and then click **OK**.
6. Select the following values , and then click **Save**:

Options	Value
SSO Protocol List	HTTP POST
User Identifier	User's Email Address
contained in	NameID

> **Note:** You must select User's Email Address option for User Identifier when JDE is configured with long user ID and select User ID when JDE is configured with short user ID.

7. Click **Export Metadata**, and then select the **Provider Metadata** option to save the SP SAML 2.0 metadata file on your computer.

Adding the Content and Experience Cloud Service Provider as a Partner in the On-Premise Identity Provider

1. Log in to the OAM Console.
2. Click **Enable SSO**, and then click **OK**.
3. Click **Federation**, and then click the **Identity Provider Management** tab.
4. Click **Create Service Provider Partner**.
5. On the new tab, type a name for the service provider partner in the Name field.
6. Click **Load Metadata**, and then click **Choose File**.
7. On the Browse window, select the SP SAML 2.0 metadata file you recently saved on your computer, and then click **Open**.
8. Select the Email Address option from the NameID Format list.
9. Select the User ID Store Attribute option from the NameID Value list.
10. Type the email address in the adjacent box, and then click **Save**.
11. Log out from the OAM.

Testing the Federation SSO

1. Log in to the MyServices Admin Console/Dashboard.
2. Click **Users**, and then click the **SSO Configuration** tab.
3. Click **Test**, and then click **Start SSO**.

   The system redirects you to the on-premise Identity Provider.
4. Use the credentials of the test user to sign in.

   If the credentials are validated, the system grants access to Content and Experience Cloud. You have successfully configured single sign-on.

17 Setting Up JD Edwards EnterpriseOne Single Sign-On Through Oracle Access Management 12c

Understanding JD Edwards EnterpriseOne Single Sign-On Through Oracle Access Management 12c

Oracle Access Management (OAM) provides single sign-on functionality for Oracle applications, including JD Edwards EnterpriseOne. It provides a secure internet infrastructure for identity management for EnterpriseOne applications and processes.

For more information, see *Understanding JD Edwards EnterpriseOne Single Sign-On Through Oracle Access Management*.

Prerequisites

In addition to single sign-on configuration instructions, this chapter contains instructions on how to install Oracle Identity and Access Management 12c, which requires the following prerequisites:

- Obtain the JDK 1.8 update 131 or later, and the Oracle Identity and Access Management installation images from the Oracle Software Delivery Cloud.
- Install Oracle Fusion Middleware Infrastructure 12c followed by OAM 12c and Oracle WebLogic Server.

Installing Oracle Identity and Access Management

This section provides basic installation instructions to support a single sign-on configuration for EnterpriseOne. If your configuration requires supporting additional applications, see the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management.*

See *Installing Oracle Identity and Access Management* for steps to install Oracle Identity and Access Management.

Setting Up OAM to Support an EnterpriseOne Single Sign-on Configuration

After installing Oracle Identity and Access Management, perform the following tasks:

- *Creating a New OAM Domain*
- *Registering the WebGate Agent for JD Edwards EnterpriseOne HTML Server*
- *Creating Additional Authentication Policies and Resource*
- *Configuring the EnterpriseOne SSO Parameter*
- *Copying the WebGate Artifact to the Oracle HTTP Server*
- *Configuring Oracle HTTP Server for the EnterpriseOne HTML Server*
- *Configuring Oracle HTTP Server for the EnterpriseOne HTML Server with SSL Ports*

Creating a New OAM Domain

To create a new OAM domain:

1. Launch config.sh (.cmd) from the `MW_Home/Oracle_common/common/bin` directory.
2. Select the required Oracle Access Manager option. The other required products are selected automatically.
3. Enter the product templates for creating the domain.
4. Enter the domain name.
5. Enter the administrator user name and password.
6. Select Production Mode or Development Mode and verify the JDK location.
7. On the Database Configure Type for Connection Parameters, enter Host Name, DBMS/Service, Port, Schema Owner, and Schema Password. Click Get RCU Configuration for checking the connection.
8. Click Next to verify the connection.
9. Select Administration Server, Node Manager, and Topology based on your requirements. See *Installing and Configuring Oracle Identity and Access Management Guide.*
10. Select Administration Server and then select Node Manager. You can accept the default values for the Administration Server and Port.
11. Select the Node Manager Type and enter its credentials.
12. Review the configuration summary and click **Create**.
13. Click **Finish** when complete.

Before you start the WebLogic Administration Console, complete the steps in the remaining tasks in this section.

Registering the WebGate Agent for JD Edwards EnterpriseOne HTML Server

1. Sign in to Oracle Access Management Console.
2. Open the Oracle Access Management Console, for example, `http://oamserver:oamport/oamconsole`.
3. Enter the Admin user name and password.
4. On the Launch Pad, select the **SSO Agent Registration** from the Quick Start Wizards section.
5. Select your WebGate and click **Next**.
6. In the Configuration section, enter a name, description, and base URL for the WebGate.

7. In the Security Option area, select the **Open** option, and then click **Finish**.

   If successful, the system displays a confirmation message and shows the location in which the artifacts are stored. Entries are also created for the new WebGate under the Host Identifiers and Application Domains nodes.
8. To see the entry under Host Identifiers, on the Launch Pad, open the Host Identifiers from the Access Manager section, and then click **Search**.

   OAM displays a list of host identifiers.
9. To see the entry under Application Domains, on the Launch Pad, open the Application Domains from the Access Manager section, and then click Search.

   OAM displays a list of application domains.

Creating Additional Authentication Policies and Resource

See *Creating Additional Authentication Policies and Resource*.

Configuring the EnterpriseOne SSO Parameter

See *Configuring the EnterpriseOne SSO Parameter*.

Copying the WebGate Artifact to the Oracle HTTP Server

After registering the SSO agent, verify the cwallet.sso and OBAccessClient.xml files have been created in the following directory:

```
<MW_Home>/user_projects/domain/<oamdomain>/output/<SSO_Agent_Name>
```

Copy files to OHS instance. For example:

```
<MW_Home>/user_projects/domain/<oamdomain>/config/fmwconfig/components/OHS/instances/<ohs_instance_name>/
webgate/config
```

Configuring Oracle HTTP Server for the EnterpriseOne HTML Server

After you install and configure the Oracle HTTP Server and Oracle HTTP WebGate, you will need to configure the mod_wl_ohs.conf file.

To configure the mod_wl_ohs.conf file:

1. Navigate to the mod_wl_ohs.conf file located at:

   ```
   <MW_Home>/user_projects/domain/<oamdomain>/config/fmwconfig/components/OHS/
   instances/<ohs_instance_name>/
   ```

2. Edit the mod_wl_ohs.conf file.

   a. Add a Virtual Host section.

```
NameVirtualHost *:7777
<VirtualHost *:7777>
  <Location /jde>   <--EnterpriseOne Context
    SetHandler weblogic-handler
    WebLogicHost myserver.com
    WebLogicPort 9003  <-- EnterpriseOne Port
  </Location>
</VirtualHost>
```

   b. If you prefer to use the single signon for the WebLogic console, then include a <Location /console> section.

```
<Location /console>  <--WebLogic Console Configuration (optional)
    SetHandler weblogic-handler
    WebLogicHost myserver.com
    WebLogicPort 9001
</Location>
```

   c. This step applies only to Oracle Access Management (OAM) for Application Development Framework (ADF) Container.

      If a virtual host section already exists for EnterpriseOne, you only need to add the Location section under the same Virtual Host section.

      For JAS, add a Virtual Host section for ADF container:

```
NameVirtualHost *:7778
<VirtualHost *:7778>
  <Location /JDEADFContainer>   <--ADF Container
    SetHandler weblogic-handler
    WebLogicHost myserver.com
    WebLogicPort 9104  <-- ADF Container Port
  </Location>
</VirtualHost>
```

      For information about the configuration settings for JAS, ADF, AIS Cookies, and ADF settings using Server Manager, see "Configuring Oracle Access Management (OAM) for ADF Container" in the *JD Edwards EnterpriseOne Tools Developer's Guide for EnterpriseOne Application Development Framework (ADF) Applications*.

Note: The HTTP port number (for example: 7777) will be the SSO port.

3. Restart the HTTP server.

   a. Change the directory to Webtier's instance. For example, **`<MW_Home>/user_projects/domain/<oamdomain>/bin`**
   b. Run **`./stopComponent <ohs_instance_name>`**
   c. Run **`./startComponent <ohs_instance_name>`**

Configuring Oracle HTTP Server for the EnterpriseOne HTML Server with SSL Ports

To achieve end-to-end secured communication from OHS to JDE E1 web client:

1. Enable SSL listen port of WebLogic managed server on which the application resides:
   a. Create a new key store to generate CA certificate.
   b. Export a certificate signing request (CSR), download and install a CA certificate along with the chain certificates into the key store created.
   c. Configure the identity and trust key stores for the WebLogic server.
2. Enable SSL communication on OHS:
   a. Create a new wallet for OHS.
   b. Generate a private key, export a certificate signing request (CSR), and download and install a CA certificate along with the chain certificates into the key store created.
   c. Ensure that the ssl.conf file has HTTPS port enabled. By default, 4443 is enabled.
   d. Import the SSL chain certificates of the web application as trusted certificates in the OHS wallet.
3. Import SSL certificates of OHS as trusted certificates in the WLS key store.
4. Import SSL certificates of OHS as trusted certificates in the Java Standard Trust key store.
5. After configuring the key store for the WebLogic managed server where HTML is deployed, select the corresponding managed server from the Weblogic Admin Console and **Restart SSL**.
6. After configuring key store and wallet, follow these steps to configure the mod_wl_ohs.conf file:
   a. Navigate to the mod_wl_ohs.conf file located at **`<MW_Home>/user_projects/domain/<oamdomain>/config/fmwconfig/components/OHS/instances/<ohs_instance_name>/`**.
   b. Edit the mod_wl_ohs.conf file.

      i. Add a location section:

```
<Location/jde> <-- EnterpriseOne Context
SetHandler weblogic-handler
WebLogicHost myserver.com
WebLogicPort 9003  <-- EnterpriseOne HTTPS Port
Debug ALL
SecureProxy ON
WlSSLWallet "OHS_wallet_location" <-- Wallet created in step 2
</Location>
```

   > **Note:** Ensure that the ssl.conf file has the HTTPS port enabled. By default, the 4443 is enabled. This will be the SSO port.

7. Restart the HTTP server.
   a. Change the directory to **`<MW_Home>/user_projects/domain/<oamdomain>/bin`**.
   b. Run **`./stopComponent <ohs_instance_name>`**
   c. Run **`./startComponent <ohs_instance_name>`**

Setting Up EnterpriseOne for Single Sign-On Integration with OAM

To set up the EnterpriseOne HTML Server for single sign-on integration with OAM through EnterpriseOne Server Manager:

1. Open Server Manager from a web browser.
2. Select your EnterpriseOne HTML Server instance.
3. In the Configuration section, select **Security Settings**.
4. In the Security Server Configuration section, select the **Enable Oracle Access Manager** option.
5. Enter the Oracle Access Manager (OAM) sign-off URL. This sign-off URL should include the OAM server URL, for example:

   ```
   http://OAMServer:OHSPort/oamsso/logout.html?end_url=http://OAMServer:OHSPort/jde/index.jsp
   ```

   Also, you can find the sign-off URL in the SSO agent that you set up in the OAM Console, as described in *Registering the WebGate Agent for JD Edwards EnterpriseOne HTML Server*. In the OAM Console, select **SSO Agents** and then search for and open the SSO agent. The sign-off URL is in the Logout Redirect URL field.
6. Click **Apply**.
7. At the prompt, click the **Synchronize** button to synchronize the changes in all .ini files.
8. Stop and restart the EnterpriseOne HTML Server.

To set up the EnterpriseOne HTML Server for ADF with OAM through EnterpriseOne Server Manager of ADF instance:

1. Open the server manager from the web browser.
2. Select the EnterpriseOne ADF server instance.
3. In the configuration section, select **Security Settings.**
4. Add OHS host and port in the HTML server whitelist field - http://OAMServer:OHSport.
5. Click **Apply**.
6. At the prompt, click **Synchronize** button to synchronize the changes in all .ini files.
7. Stop and restart the EnterpriseOne ADF server.

Configuring SSO Support for EnterpriseOne AIS Server Clients

In an EnterpriseOne single sign-on setup through Oracle Access Manager (OAM) or Identity Cloud Service (IDCS), an additional configuration is required to support single sign-on with applications that run on the AIS Server, which include EnterpriseOne mobile enterprise applications. To support this setup, EnterpriseOne uses 2 level authorization of OAuth service from OAM 12c or IDCS. This setup is also required to support e-signatures in an EnterpriseOne SSO configuration. Follow the configuration steps in this section for either OAM or IDCS.

To configure single sign-on support with OAM for AIS clients, see:

- *Enable the "OAuth and OpenIDConnect Service" in OAM*
- *Configure OAuth Services*

- *Configure OAM Mobile Settings for the Enterprise Server in Server Manager*
- *Configuring IDCS for SSO*
- *Configure OAuth Services for IDCS*
- *Configure IDCS Settings for the HTML Server in Server Manager*

Enable the "OAuth and OpenIDConnect Service" in OAM

1. In OAM, navigate to Configuration, Available Services.
2. If not enabled, click the **OAuth and OpenIDConnect Service** to enable it.

Configure OAuth Services

Refer to REST APIs to create resources required for OAuth services OAM 12c configuration.

See `REST API for OAuth in Oracle Access Manager` for more information.

1. **Create OAuth Identity Domain -** An identity domain corresponds to the notion of a tenant. All clients and resource servers are created under the identity domain. You need to provide the identity store details for creating the OAuth Identity domain.

   See *Creating Identity Store in OAM Console*.
2. **Create OAuth Resource Server -** A resource server hosts protected resources. The resource server is capable of accepting and responding to protected resource requests using access tokens. It should refer to the above identity domain.
3. **Create OAuth Client -** A client is an application that makes protected resource requests on behalf of the resource owner. The ClientID and the ClientName should be same.

Configure OAM Mobile Settings for the HTML Server in Server Manager

1. In Server Manager, access the Security Server Configuration settings for the HTML Server.
2. Make sure that the **Enable Oracle Access Manager** check box is selected.
3. Select the setting **Oracle Access Manager Version or IDCS**.
4. Complete the following fields:
   - **Oracle Access Manager Mobile Service Domain Name** Enter the Identity Domain Name created using OAuth Service in OAM 12c.
   - **OAuth Resource Server Scope** Enter the Resource Server Scope for which OAuth Client has been created.
   - **OAuth ClientId** Enter the OAuth ClientID created for the Identity Domain and Resource Server Scope.
   - **OAuth Secret** Enter the Secret of the ClientID created for the Identity Domain and Resource Server Scope.
   - **OAuth Authentication URL** Enter the URL for creating Access Token from OAuth 12c Runtime API.
   - **OAuth Validation URL** Enter the URL for validating Access Tokens from OAuth 12c Runtime API.

   The Oracle Access Manager Sign-Off URL setting is only for EnterpriseOne web client applications. You can ignore it for this configuration.

5. Complete the configuration by performing the steps in the following sections, after which users can use their single sign-on user name and password to sign on to EnterpriseOne mobile applications.

Configure IDCS for SSO

Using the IDCS Administrative Console you must configure the OAuth Configuration tab of the JDE Application used for single sign-on. The EnterpriseOne SSO integration with IDCS uses the Resource Owner Password Credentials Grant provided by IDCS (see doc *https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/ocuid/resource-owner-password-credentials-grant.html*). The steps below describe the configuration for this type of authentication in IDCS.

For more information on the REST APIs in IDCS see:

https://docs.oracle.com/en/cloud/paas/identity-cloud/rest-api/api-oauth-runtime-oauth-runtime-tokens.html

https://docs.oracle.com/en/cloud/paas/identity-cloud/rest-api/op-oauth2-v1-introspect-post.html

All configurations below should be done on the existing Enterprise Application in IDCS that is used for EnterpriseOne single sign-on. It is recommended that SSO be configured and working for single sign-on before performing this additional configuration.

1. In the IDCS administrative console navigate to the JDE application and select it.
2. Navigate to the OAuth Configuration tab.
   Refer to these links to IDCS documentation for more information about OAuth configuration:
   https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/add-enterprise-application.html
   https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/understand-cloud-applications.html#GUID-29F8FC7E-DF14-4EAE-9CFF-75B125BC3FB4
3. **Generate Client ID and Secret**
   If you have not done so already in the General Information tab, choose to generate a client id and secret.
4. **Client Configuration**
   Navigate to the **Client Configuration** section.
5. In the **Allowed Grant Types** section, check the box for **Resource Owner** .
6. Check the box for **Introspect in Allowed Operations**.
7. In the **Token Issuance Policy – Resources** section, add the respective scope for this IDCS service. Make a note of the scope for use in configuration of the HTML Server, which is described in the following section.
8. Save your changes to the Application.

Configure OAuth Services for IDCS with the Content and Experience Cloud integration with JD Edwards EnterpriseOne

In addition to using the JD Edwards EnterpriseOne program P95400 to add soft coding entries, you must use Server Manager configure the following IDCS properties.

1. In the Server Manager Console, select an HTML Server instance, Configuration (left side panel), Advanced (from the drop-down menu, Security.
2. **Oracle Access Manager Version or IDCS**
   Use the drop-down menu to select **Identity Cloud Service**.

3. **OAuth Client ID**

   Enter the IDCS application client id.
4. **OAuth Client Secret**

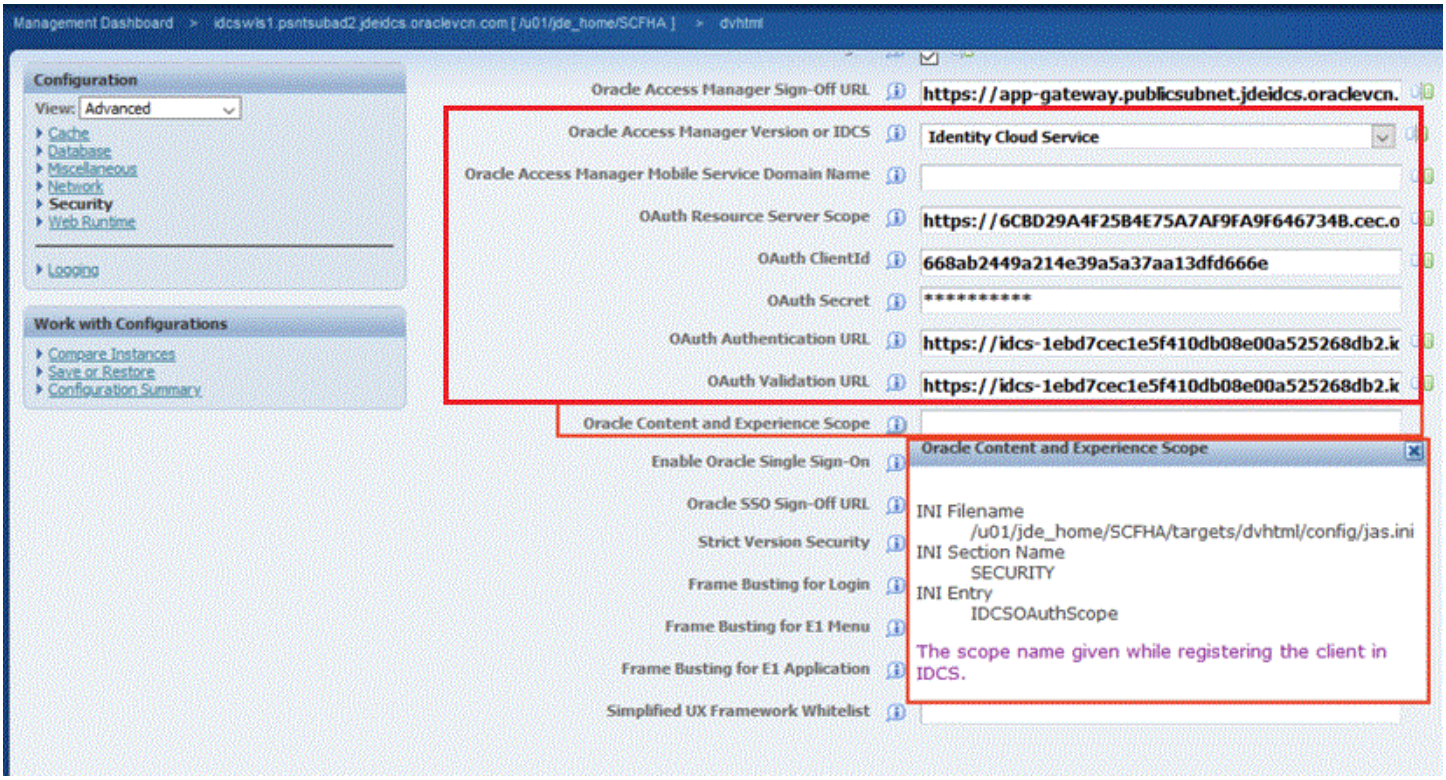
   Enter the IDCS application client secret.
5. **OAuth Authentication URL**

   Enter the URL for creating Access Token in IDCS Runtime Token API. For example:

   https://*<idcs tenantname that is protecting this service>*/oauth2/v1/token
6. **Oracle Content and Experience Scope**

   Enter the scope used in the IDCS application setup. This is scope that you specified in the proceeding section of this document for Configuring IDCS.

For example:



Configure IDCS for AIS Clients and E-Signature in the JD Edwards EnterpriseOne HTML Server in Server Manager

Use Server Manager to configure IDCS for AIS clients and E-Signature in the JD Edwards HTML Server.

1. In the Server Manager Console, select an HTML Server instance, Configuration (left side panel), Advanced (from the drop-down menu, Security.
2. Ensure the **Enable Oracle Access Manager** check box is selected.
3. For **Oracle Access Manager Version or IDCS**, use the pull-down menu to select **Identity Cloud Service**.
4. Complete the following fields:
   - **OAuth Resource Server Scope:**

     Enter the Scope used in the IDCS application setup.
   - **OAuth ClientId:**

     Enter the IDCS application client id.
   - **OAuth Secret:**

     Enter the IDCS application client secret.
   - **OAuth Authentication URL:**

     Enter the URL for creating Access Token in IDCS Runtime Token API. (for example: "https://%3cIDCS-Service-Instance%3e.identity.oraclecloud.com/oauth2/v1/token")
   - **OAuth Validation URL:**

     Enter the URL for validating Access Token from in IDCS Runtime Introspect API.(for example:https://%3cIDCS-Service-Instance%3e.identity.oraclecloud.com/oauth2/v1/introspect")
5. Complete the configuration by performing the steps in the following sections, after which you can use your single sign-on user name and password to sign on to EnterpriseOne mobile applications or perform e-signatures in EntepriseOne.

Adding JD Edwards EnterpriseOne HTML Server User to the OID

Oracle Directory Services Manager (ODSM) is required to add a valid JD Edwards EnterpriseOne web client user to Oracle Internet Directory (OID).

See *Adding JD Edwards EnterpriseOne HTML Server User to the OID* for more information on steps to add a user to OID.

Creating Identity Store in OAM Console

See *Creating Identity Store in OAM Console*.

Testing the Sign-On Configuration

See *Testing the Single Sign-On Configuration*.

Configuring Federation SSO in Content and Experience Cloud (Release 9.2.2 Update)

See *Configuring Federation SSO in Content and Experience Cloud (Release 9.2.2 Update)*.

Detaching Credential Collector Configuration

The detached credential collector (DCC) configuration is a logical part of the OAM server and acts as a front-channel communication endpoint of the OAM server. It submits the credential request directly to the Webgate, while in ECC, the credential request is submitted to the OAM server.

The detached credential collector also:

- Stands alone, that is, it is detached from the OAM server and does not require an application server.
- Supports RSA SecurID pass code verification.
- Works similar to the Authenticating Webgate with greater flexibility for server scale-out and attack resilience, credential collection UI construction, flow, and life cycle management.

The detached credential collector was introduced in OAM 11gR2 release and it is further extended to OAM 12c.

Enabling Credential Operations for an Existing 12c Webgate

Using the Oracle Access Management Console:

1. Click Agents and then click Search to open the 12c webgate page that functions as the DCC.
2. Select the check box Allow Credential Collector Operations.
3. Click Apply and download the webgate zip file.
4. Place the webpage zip file at two locations:
   - MW_HOME /user_projects/domains/oam_domain/output/E1OHS12cWebgate/
   - MW_HOME /user_projects/domains/oam_domain/config/fmwconfig/components/OHS/instances/ohs1/webgate/config/

     Take backup of the existing "cwallet.sso , cwallet.sso.lck, ObAccessClient.xml and wallet" and unzip the downloaded webgate zip file.

Verifying the Perl Executable

Make sure that the path name of the perl executable is correct. This can be done by comparing the perl executable path name with the path name mentioned in the perl scripts.

To ensure that the perl script mentions the correct path for the perl executable

1. Use 'which perl' command to verify the perl path.
2. Change the first line of the perl scripts (login.pl, logout.pl, securid.pl) to make it point to the correct location. For example, replace it with MW_HOME/perl/bin/perl.

   If the webgate is installed at MW_HOME/webgate, the perl scripts for DCC-based login can be located at MW_HOME/webgate/ohs/oamsso-bin.

Configuring the Authentication Scheme for DCC

Configure a new authentication scheme:

1. Click Authentication Scheme.
2. Click + to add a new authentication scheme.
3. On clicking + a new page opens where you can add the new authentication scheme. Fill up the following fields as:

   - Name: DCCAuthScheme

     The name can be anything with no spaces.
   - Authentication Level: 2
   - Challenge Method: FORM
   - Challenge Redirect URL: http://<OAM_SERVER>:<OHS_port>

     Enter the OHS server URL here where you have configured the webgate for the DCC.
   - Authentication Module: LDAP
   - Challenge URL: /oamsso-bin/login.pl
   - Context Type: Select the external

   Click Apply.

Configuring the Authentication Policy for the Protected Resource

1. Go to the Authentication Policy, Protected Resource Policy and choose 'DCCAuthScheme' as the authentication scheme.
2. Restart the OAM server and check the confguration. Access the page via http://<OAM_SERVER>:<OHS_port>/jde/E1Menu.maf. This navigates you to the login page.

Configuring the Sign-Off URL for the EnterpriseOne Server Manager

1. Login to the EnterpriseOne Server Manager.
2. Open the JDE E1 HTML Server instance by using single sign on.
3. Select Enable Oracle Access Manager checkbox.
4. Enter below value for Oracle Access Manager Sign-Off URL:

   http://<oam_server>:<OHS_port>/oamsso-bin/logout.pl?end_url=http://<oam_server>:<OHS_port>/oamsso-bin/login.pl
5. Click **Apply**.
6. At the prompt, click the **Synchronize** button to synchronize the changes in all .ini files.
7. Stop and restart the EnterpriseOne HTML Server.

18 Using Oracle Access Manager to Enable Support for Windows Native Authentication with EnterpriseOne

Using Oracle Access Manager to Enable Support for Windows Native Authentication with EnterpriseOne

This chapter includes instructions in support of Oracle Access Manager 11g Release 1 (OAM 11gR1) and 11g Release 2 (OAM 11gR2). For OAM 11gR2, Oracle Access Manager has been renamed to Oracle Access Management. When necessary, this chapter contains explicit instructions for each version of OAM.

Understanding Windows Native Authentication Support in OAM

OAM enables users to automatically authenticate to their web applications, including EnterpriseOne web client applications, using their desktop credentials. This is known as Windows Native Authentication (WNA). This configuration requires storing user credentials in a Windows Active Directory instance that is registered as a user-identity store in OAM.

Note: You can enable support of long user IDs and passwords in a JD Edwards EnterpriseOne single sign-on configuration with OAM. See *Configuring Long User ID and Password Support in a Single Sign-On Configuration with Oracle Access Manager* in this guide for more information.

Before You Begin

Before following the instructions in this chapter, make sure that you have:

- A fully-configured Active Directory authentication service.
- An EnterpriseOne HTML Server.
- A SSO/OAM (including Oracle HTTP Server and WebGate) configuration with your EnterpriseOne web client applications.
- A record of the domain names and the server's fully qualified domain names.
- Synchronized clocks between Active Directory and OAM servers.

Performing Prerequisite Integration Tasks

This section describes the integration tasks that you must complete before configuring OAM to use Windows Native Authentication. The integration tasks include:

- **For Oracle Identity and Access Management 11gR1 only**: Installing the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy File version of the JDK that is configured in the OAM WebLogic Server domain.
  For JDK 6:
  `http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html`
  For JDK 7: `http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html`
- *Creating an Active Directory User*
- *Editing the krb5.conf (ini) File on the OAM Server*
- *Creating a Service Principal Name (SPN) from the Active Directory Machine*
- *Obtaining the Kerberos Ticket*

Creating an Active Directory User

To create an active directory user:

1. Log on to the Active Directory server.
2. Use the "Active Directory Users and Computers" application to create an Active Directory user ID.
3. Record the user name—both the sAMAccountName and userPrincipalName—and password.

Editing the krb5.conf (ini) File on the OAM Server

1. Open the krb5.conf (ini) file, which is normally located in `/etc/krb5.conf` or `C:\Windows\krb5.ini`.
2. Update the file with your Active Directory domain information. If the file does not exist, use the following entries to create it:

```
[libdefaults]
default_realm=JDELDAP.COM
default_tkt_enctypes=RC4-HMAC
default_tgs_enctypes=RC4-HMAC
ticket_lifetime=600
clock_skew = 600

[realms]
JDELDAP.COM = {
 kdc = denjdeldap1.jdeldap.com
 admin_server = denjdeldap1.jdeldap.com
 default_domain = JDELDAP.COM
 }

[domain_realm]
 .jdeldap.com = JDELDAP.COM
 jdeldap.com = JDELDAP.COM
```

Creating a Service Principal Name (SPN) from the Active Directory Machine

1. Run the following command to create a service principal name (SPN):

   >setspn -S HTTP/OAM_Server ActiveDirectoryUserID

   > **Note:** You can use the "-A" option, but "-S" checks for a duplicate SPN as shown in the following example. In the examples, JDE is the Active Directory user ID.

```
C:\Windows\system32>setspn -s HTTP/yourdomain.com JDE
Checking domain DC=jdeldap,DC=com

Registering ServicePrincipalNames for CN=JDE,CN=Users,DC=jdeldap,DC=com
        HTTP/yourdomain.com
Updated object
```

2. Run the "ktpass" command to create the SPN and associate it with the Active Directory user ID that you created.

   ktpass -princ HTTP/yourdomain.com@JDELDAP.COM -mapuser ActiveDirectoryUserID -pass ###### -out C:\jde105.keytab -ptype KRB5_NT_PRINCIPAL -crypto ALL

```
C:\Windows\system32>ktpass -princ HTTP/yourdomain.com@JDELDAP.COM -mapuser JDE -pass XXXXXX1
   -out c:\jde105.keytab -ptype KRB5_NT_PRINCIPAL
Targeting domain controller: denjdeldap1.jdeldap.com
Using legacy password setting method
Successfully mapped HTTP/yourdomain.com to JDE
Key created.
Output keytab to c:\jde105.keytab:
Keytab version: 0x502
keysize 75 HTTP/yourdomain.com@JDELDAP.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 5 etype 0x17 (RC
4-HMAC) keylength 16 (0xe45a314c664d40a227f9540121d1a29d)
```

3. To verify that the SPN and the Key Tab file are set up correctly, view the user information from Active Directory, as shown in the following example:

sAMAccountName	JDE
sAMAccountType	< samUserAccount >
userPrincipalName	HTTP/yourdomain.com@JDELDAP.COM
lockoutTime	unspecified
servicePrincipalName	HTTP/yourdomain.com

   You can also use the "setspn" command to view the user information:

   >setspn -L ActiveDirectoryUserID

```
C:\Windows\system32>setspn -L JDE
Registered ServicePrincipalNames for CN=JDE,CN=Users,DC=jdeldap,DC=com:
        HTTP/yourdomain.com
```

4. Use the following command to remove the SPN:

   >setspn -D "SPN" ActiveDirectoryUserID

```
C:\Windows\system32>setspn -d HTTP/dnptlx105. <domain> .com JDE
Unregistering ServicePrincipalNames for CN=JDE,CN=Users,DC=jdeldap,DC=com
        HTTP/yourdomain.com
Updated object
```

5. After verifying the setup of the SPN and the Key Tab, copy the Key Tab file to the OAM server.

Obtaining the Kerberos Ticket

1. On the OAM host machine, run this command from **JDK_HOME/bin**:

   kinit.exe -k -t <Full_Path_To_KEYTAB_File> <Service_Principal_Name>

   After running the command, the system should display "**Authenticated to Kerberos v5**".
2. Run the "**klist -e**" command to check the ticket:

```
Ticket cache: FILE:/tmp/krb5cc_501
Default principal: HTTP/yourdomain.com@JDELDAP.COM
Valid starting     Expires            Service principal
07/10/13 14:30:22  07/10/13 14:40:22  krbtgt/JDELDAP.COM@JDELDAP.COM
        Etype (skey, tkt): ArcFour with HMAC/md5, AES-256 CTS mode with 96-bit
 SHA-1 HMAC
        Kerberos 4 ticket cache: /tmp/tkt501
klist: You have no tickets cached
```

This concludes the initial integration steps for Active Directory and Kerberos. If "klist" and "kinit" commands are not successful, resolve the issue before continuing.

Configuring OAM to Use Windows Native Authentication

1. Log in to OAM Admin Console: http://host:port/oamconsole.

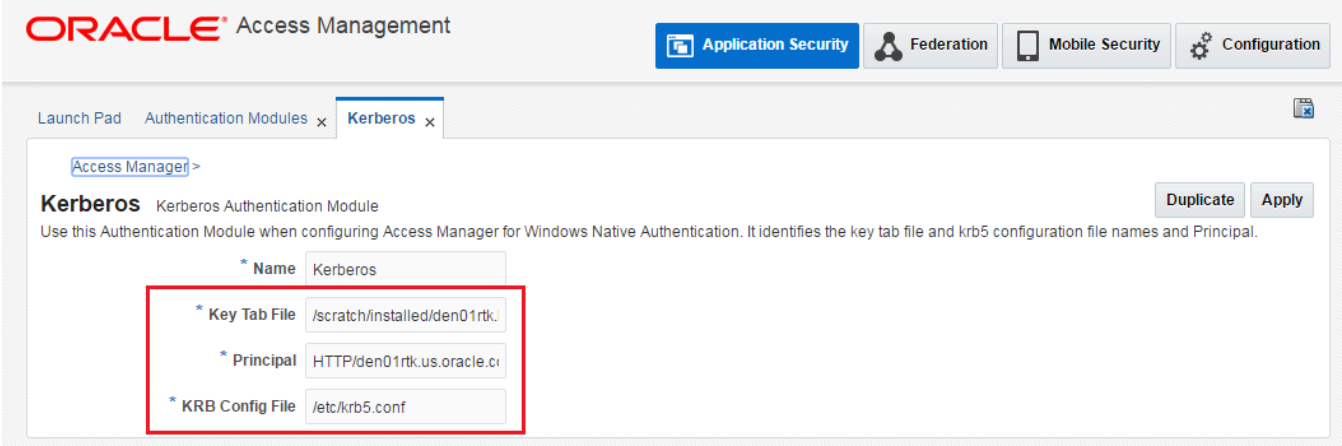
   For OAM 11gR2, the Admin Console is called the Oracle Access Management console.

2. Create an Active Directory data source and set it as the Default Store:

   For OAM 11gR1: On the System Configuration tab, expand the Data Sources folder, select user identity Stores, and then click the Create button.

   For OAM 11gR2: Select the User Identity Store from the configuration area, and the click the Create button.

   a. When you create the data source, select the **Default Store** option to make it the default identity store.
   b. Click the **Apply** button.
   c. Click the **Test Connection** button to test the configuration.



3. Update the Kerberos Authentication Module:

   For OAM 11gR1: On the System Configuration tab, select the **Access Manager Settings** pane. Expand the **Authentication Modules** node, **Kerberos Authentication** module, and then double-click **Kerberos**.

   For OAM 11gR2: Select the **Authentication Modules** from the Access Manager area, click **Search**, and select **Kerberos Module**.

   a. Complete the following fields to enter the location of your Key Tab and krb5.conf (ini) files:

      Key Tab File: Enter /u01/OracleOAM/Middleware/jde_wna\mad08.keytab

      Principal: Enter HTTP/*yourdomain*.com@JDELDAP.COM

      KRB Config File: Enter /etc/krb5.conf (C:\Windows\krb5.ini)
   b. Click the **Apply** button.

4. Verify that the authentication scheme is using the correct Kerberos authentication module you modified in the previous step:

   For OAM 11gR1: Select the **Policy Configuration** tab. Under the Authentication Schemes node, double-click **KerberosScheme**.

   For OAM 11gR2: Select **Authentication Schemes** from the Access Manager area. Click **Search** and then double-click **KerberosScheme**.
5. Edit the Protected Resource Policy:

   For OAM 11gR1: Expand the **Application Domains** node, the domain node, **Authentication Policies**, and then double-click **Protected Resource Policy**.

   For OAM 11gR2: Select the Application Domain from the Access Manager area and then click **Search**. Select your domain node from the Authentication Policies, and then double-click **Protected Resource Policy**.
   a. In the Authentication Policy area, edit the Protected Resource Policy by selecting **KerberosScheme** for the Authentication Scheme.
   b. Click the **Apply** button.

Enabling the Browser to Return Kerberos Tokens

To configure browsers to return Kerberos tokens:

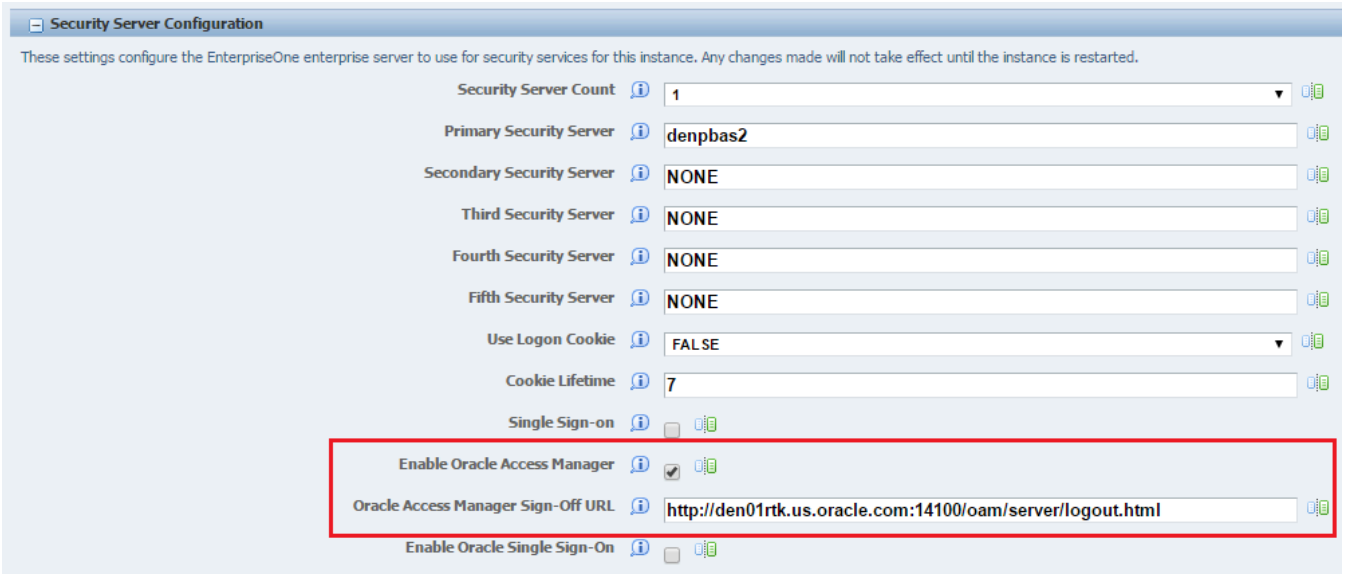
1. Right-click the Windows Start button and select Search.
2. Enter Internet Options in the Search field.
3. In the search results, click Internet Options Control Panel.
4. Click the Security tab.
5. Select Local as the intranet option.
6. Click the Sites button.
7. Click the Advanced button.
8. Add the OAM host or domain name.
9. Click Close.
10. Click OK.
11. Click the Custom level button.
12. Scroll down to the Scripting section.
13. Under Active Scripting, click the Enable option.
14. Scroll down to the User Authentication section.
15. Under logon click the Automatic button only in Intranet Zone section.
16. Click OK.
17. Select the Advanced tab.
18. Scroll down to the Security section.
19. Select the option Enable Integrated Windows Authentication.
20. Click OK.

Modify the EnterpriseOne ini Setting

After completing the configuration, modify the EnterpriseOne ini setting so that users are not returned to the sign-in screen after signing out of EnterpriseOne.

1. Sign in to EnterpriseOne Server Manager.
2. Select your EnterpriseOne HTML server.

3. In the Configuration area, select Security Settings.



4. Under the Security Server Configuration section, in the Oracle Access Manager Sign-Off URL field, remove the rest of the information starting with "`?end_url=`". Only the OAM server URL should remain, as shown in the following examples:

   Example of a sign-off URL in OAM 11gR1:

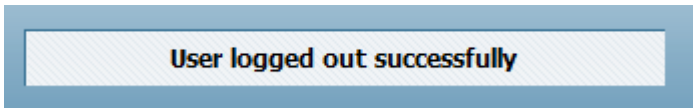
   ```
   http://server:port/oamsso/logout.html
   ```

   Example of sign-off URL in OAM 11gR2:

   ```
   http://server:port/oam/server/logout.html
   ```

   Also, you can find the sign-off URL in the SSO agent that you set up in the OAM Console, as described in *Registering the WebGate Agent for JD Edwards EnterpriseOne HTML Server*. In the OAM Console, select SSO Agents and then search for and open the SSO agent. The sign-off URL is in the Logout Redirect URL field.

   When logging out, a message stating "User logged out successfully" appears.



5. Restart the server.

Validating the Windows Native Authentication Configuration

To validate the Windows Native Authentication configuration:

1. Log on to a Windows system as an Active Directory domain user.
2. Open a browser and launch the EnterpriseOne web client.

   If the configuration was successful, you should be able to access the EnterpriseOne web client without being prompted for credentials.

19 Configuring Long User ID and Password Support in a Single Sign-On Configuration with Oracle Access Manager

Configuring Long User ID and Password Support in a Single Sign-On Configuration with Oracle Access Manager

This chapter describes how to use Oracle Access Manager (OAM) to configure support of long user IDs and passwords in a JD Edwards EnterpriseOne single sign-on configuration.

Understanding Long User ID and Password Support for EnterpriseOne through OAM

Note: Starting with EnterpriseOne Tools 9.2, you have the OPTION to enable the Long User feature and Long Password feature in EnterpriseOne. If you do not enable the Long User and Long Password features in EnterpriseOne Tools 9.2, you can still set up long user IDs and passwords with OAM in an EnterpriseOne single sign-on configuration.

As with releases prior to EnterpriseOne Tools 9.2, out of the box, EnterpriseOne user IDs are limited to 10 characters. Using OAM, you can manage long user IDs and passwords in a single sign-on configuration with EnterpriseOne. This configuration does not change the behavior of existing EnterpriseOne user IDs, but it requires mapping EnterpriseOne users to the long IDs.

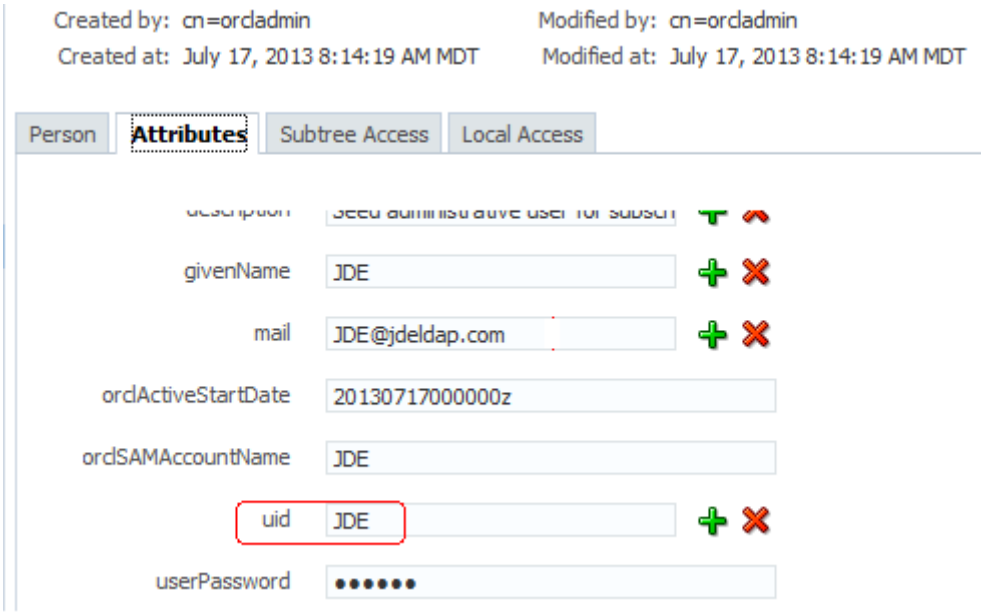
Prerequisites

Make sure the following software is properly configured:

- Oracle Internet Directory (OID)
- Oracle Identity and Access Management
- Oracle HTTP Server (WebTier) and WebGate
- OAM agent and single sign-on between OAM and EnterpriseOne

Configuring LDAP for Longer User IDs

1. Log in to Oracle Internet Directory, for example: http://host:*port*/odsm
2. Create a user account:
   a. In the tree in the left pane, expand the Root node, dc=com, dc=mycompany.
   b. Click the **Create** icon.



   c. If you are planning to use an email address for your user ID, record the information in the "uid" attribute.
3. Log out and close Oracle Directory Manager.

> **Note:** If you are using Active Directory, use "userPrincipalName" as the "mail' attribute and "sAMAccountName" as the "uid" attribute.

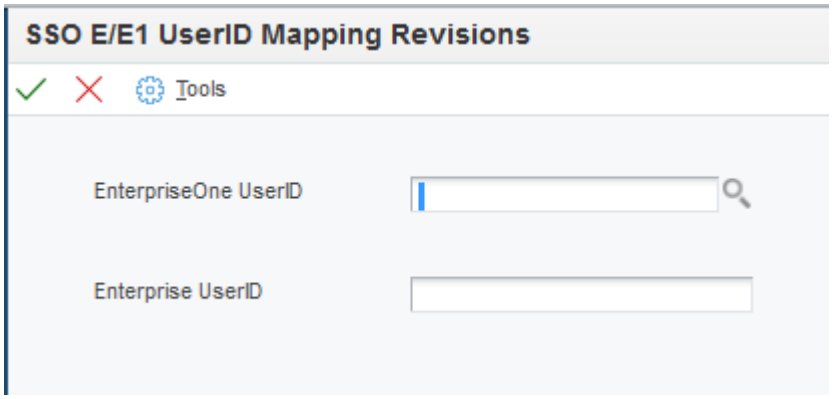
Creating a User Mapping in EnterpriseOne

> **Note:** The application for mapping EnterpriseOne user IDs is available only on the EnterpriseOne Windows client.

1. Sign in to the EnterpriseOne Windows client.

2. Select the **System Administration Tools** menu (GH9011), **Security Maintenance**, **Security Maintenance Advanced and Technical Operations**, and then double-click **SSO Environment Configuration Tools**.

3. On SSO Environment Configuration Tools, select the **Configure the UserID Mapping** link.
4. On Work With SSO E/E1 UserID Mapping, click the **Add** button.



5. On SSO E/E1 UserID Mapping Revisions, complete these fields:
   - **EnterpriseOne UserID**. Enter the existing EnterpriseOne user ID.
   - **Enterprise UserID**. Enter the new long user ID created in LDAP.

     This is the same as the user ID entered in the "mail" field in OID or "userPrincipalName" in Active Directory.

   Note: All entries MUST be entered in upper case.

   EnterpriseOne saves the information in the F00927 table as shown in the following screenshot:

EnterpriseOneID	EnterpriseID	EnterpriseOne Address Number	EnterpriseOne User Name
JDE	JDE@JDELDAP.COM	304881	James Black

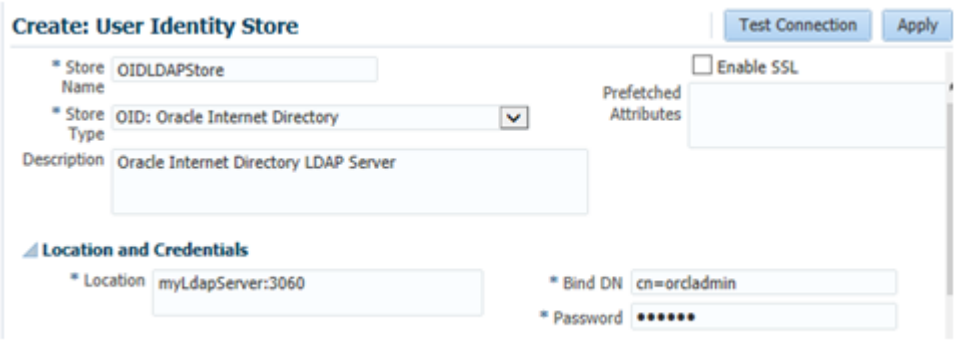
Configuring OAM for Long User IDs

Set up and configure OAM single sign-on to use a different attribute for EnterpriseOne. To do so, perform the following tasks:

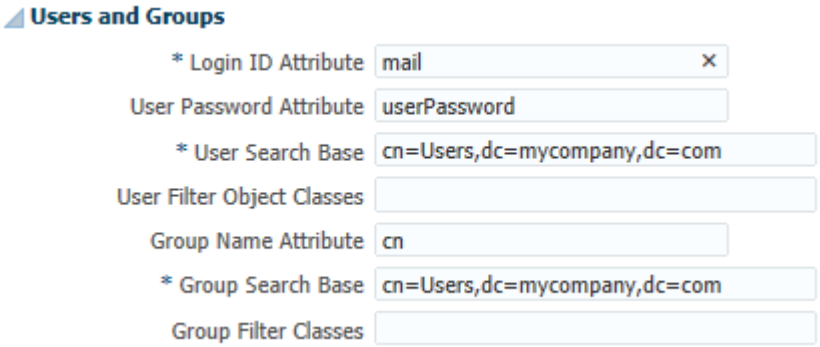
- *Creating an Identity Store*
- *Creating an Authentication Module*
- *Creating an Authentication Scheme*
- *Applying the Authentication Scheme to the Application Domain*

Creating an Identity Store

1. In the OAM Console, in the Configuration area, click the **User Identity Stores**.
2. Click the **Create** button.



3. Enter a store name and store type in the applicable fields.
4. In the *Location field, enter your LDAP Server and port.
5. In the Bind DN and Password fields, enter the credentials to the LDAP Server.
6. Click **Test Connection**.



7. In the Users and Groups area, change the User Name Attribute to use the long ID attribute, such as "mail" for OID.

   Note: Use "userPrincipalName" for Active Directory.

8. Click the **Apply** button to add the identity store.

9. In the Users and Groups area, change the User Name Attribute to use the long ID attribute, such as "mail" for OID:

   Note: Use "userPrincipalName" for Active Directory.

10. Click the **Apply** button to add the identity store.
11. Return to the User Identity Store main page and select your identity store as the Default Store.Select the Default Store option to make it the default identity store.

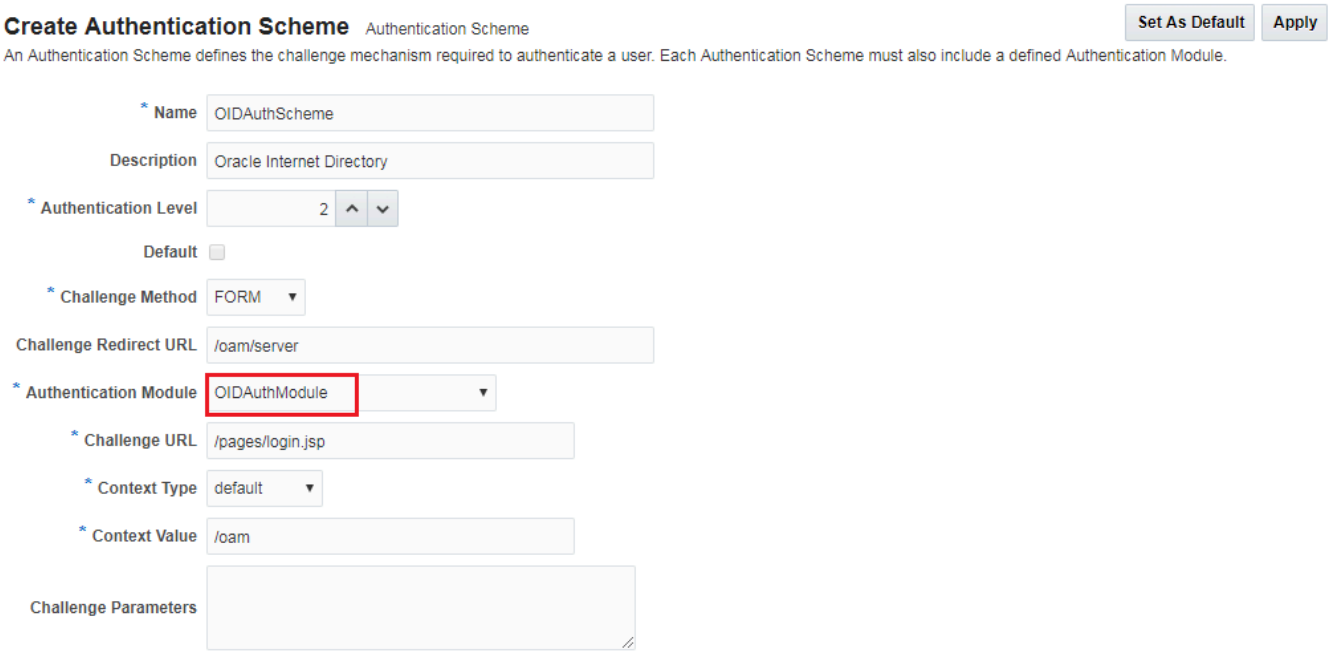
Creating an Authentication Module

1. Select the Authentication Modules from the Access Manager Area.
2. Select **Create LDAP Authentication Module** from the Create Authentication Module drop-down menu.
3. In the Name field, enter a name for the authentication module.
4. In the User Identity Store field, select the identity store that you created in the previous step.
5. Click the **Apply** button to add the authentication module.

Creating an Authentication Scheme

1. Select the Authentication Schemes from the Access Manager Area.

2. Click the **Create Authentication Scheme** button.



Applying the Authentication Scheme to the Application Domain

1. Select the Application Domains from the Access Manager area, click **Search**, and select your domain node.
2. Click the **Authentication Policies** tab, and then double-click **Protected Resource Policy**.
3. Enter the new authentication scheme.
4. Click the **Apply** button to add the authentication scheme.
5. Repeat these steps if you have more EnterpriseOne policies.

Validating the Long ID Configuration

To validate the long ID configuration, use the single sign-on URL to access EnterpriseOne and then enter the long ID, such as an email address, to sign in. If the configuration was successful, you should be able to access the EnterpriseOne web client.

20 Configuring SSL/TLS for JDENET

Understanding SSL/TLS for JDENET

Secure Sockets Layer (SSL/TLS) is a cryptographic protocol that enables secure communication between applications across a network. Enabling SSL/TLS communication provides several benefits, including message encryption, data integrity, and authentication. An encrypted message ensures confidentiality in that only authorized users have access to it. Data integrity ensures that a message is received intact without any tampering. Authentication guarantees that the person sending the message is who he or she claims to be.

You can configure EnterpriseOne to use SSL/TLS to encrypt all JDENET message data passed between the Enterprise Server and clients. In this context, a client would include an HTML Server, the Deployment Server, or any other client that makes requests to the EnterpriseOne Enterprise Server.

Installing SSL Programs on IBM System i

For the IBM System i platform, EnterpriseOne provides two SSL-based components within a save file. You have to extract these components to the system foundation IFS folder (such as E910SYS) before you can create and use SSL certificates as described in the following section, "Generating an SSL Certificate and Key File."

The following steps describe how to use the command to extract the components for SSL Programs on IBM System i:

1. Ensure the system foundation library is in your library list. If it is not in the list, you can add it by entering this command:

   ADDLIBLE *E910SYS*

   Where *E910SYS* is the name of the system foundation library.
2. From an IBM System i command line, enter the following command:

   INSTALLSSL
3. Press F4 to prompt the command.
4. Enter the name of your system foundation library, and then press Enter.

Generating an SSL/TLS Certificate and Key File

To use secure sockets, the server must have an SSL/TLS certificate and private key. This information is used by the SSL/TLS library functions to generate unique encryption keys for each connection and negotiate the secure connection with the client. EnterpriseOne provides a script file that can be used to generate a combination certificate/key file for use with SSL/TLS.

On Windows enterprise and deployment servers, the gencert.cmd file is used to generate a combination SSL/TLS certificate/private key file that is suitable for use with JDENET SSL/TLS. On UNIX and Linux systems, the file is called **gencert.sh**. On IBM System i, the command is **GENCERT**, which must be run from QSHELL. These files can be found in the **system/bin32 (or bin64)** directory on the enterprise server and also on the deployment server. The following illustration

shows an example of running the script to generate a certificate. Notice that the system prompts you to enter data that is unique to your site to create the certificate/key file:

```
C:\Windows\system32\cmd.exe
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.............++++++
...........++++++
writing new private key to 'Z:\JDEdwards\E900\DDP\system\bin32\key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Colorado
Locality Name (eg, city) []:Denver
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Oracle
Organizational Unit Name (eg, section) []:Development
Common Name (e.g. server FQDN or YOUR name) []:yourdomain.com
Email Address []:admin@oracle.com

Z:\JDEdwards\E900\DDP\system\bin32\key.pem



Z:\JDEdwards\E900\DDP\system\bin32\cert.pem


        1 file(s) moved.
Certificate file '..\..\SSL\server.pem' has been created for use with SSL.

Press any key to continue . . .
```

The file generated by this script should be entered as the sslKeyFile parameter in the enterprise or deployment server JDE.INI file when using SSL/TLS. See *Configuring the Enterprise Server JDE.INI File* in this chapter. By default, the file is created in a directory outside the main system directory to ensure that the certificate/key file is preserved during an EnterpriseOne Tools release upgrade.

More about Certificates

It is not required to generate the certificate/key file on the server that will use it. You could, for example, generate a certificate/key file on the Deployment Server and move it to your Enterprise Server when you are ready to start using SSL/TLS.

You can also use commercially signed certificates, such as certificates validated by a company like Verisign or Cybertrust, to set up SSL/TLS for JDENET, with some caveats. The EnterpriseOne enterprise and deployment servers currently require a combination certificate and key file in PEM format. In addition, the file must not be pass-phrase protected. Currently, using a commercially signed certificate with the JDENET server does not offer any advantage over using the self-signed, internally generated certificate as described in this section.

Configuring the Enterprise Server JDE.INI File

Starting with JD Edwards EnterpriseOne Tools 9.1 Update 2.1, the "Network and Queue Settings (JDENET Configuration)" section of the enterprise server JDE.INI file contains three settings for SSL/TLS support. These settings are used only by the enterprise server. Clients that connect to the enterprise server do not have any related settings, as the enterprise server tells the client the type of connection to be used. Because of this architecture, older EnterpriseOne clients that do

not support SSL/TLS cannot connect with an EnterpriseOne server that is enabled with SSL/TLS. Therefore, SSL/TLS support for JDENET requires that the release level of EnterpriseOne clients matches the release level of EnterpriseOne servers.

The SSL/TLS settings in the "Network and Queue Settings (JDENET Configuration)" section of the jde.ini include:

- useSSL

  Valid values are `Enable SSL` or `Disable SSL`. Enabling this option specifies that JDENET messages will be exchanged using secure sockets (SSL/TLS). The setting is only set on the server, but does require that clients accessing the server can process SSL/TLS messages (that is, all clients must be running with a matching EnterpriseOne Tools release). Starting with EnterpriseOne Tools 9.1 Update 2.1, Disable SSL is the default setting in EnterpriseOne Tools 9.1 Update 2.1.

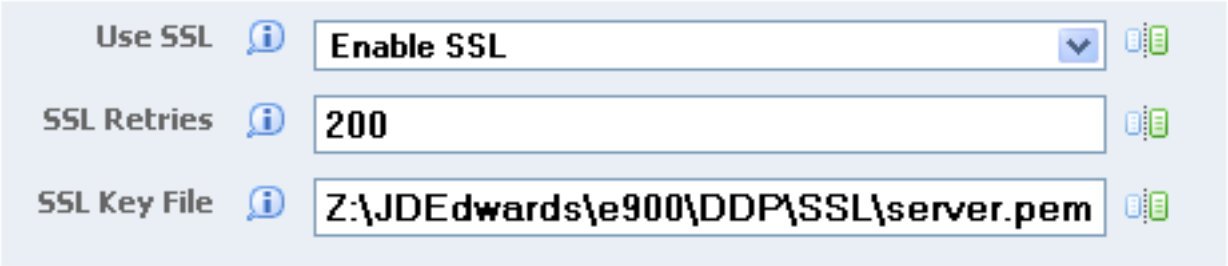
- sslRetries

  This setting specifies the maximum number of times the server or client will attempt to complete an SSL/TLS handshake. If the handshake is not completed within the retry limit, the SSL/TLS connection fails. The retry limit prevents the server from hanging on an SSL/TLS connection that may never complete. The default value of 1000 for this setting should be appropriate for most installations, but may need to be increased to allow for slow clients or high network latency.

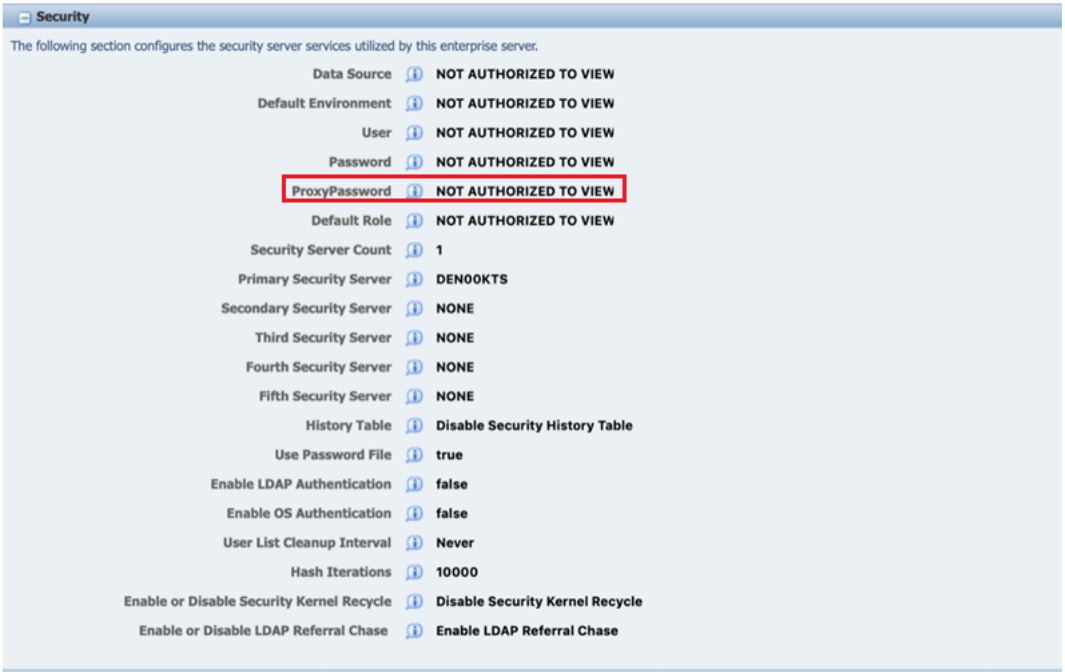
- sslKeyFile

  You must set this parameter to the fully qualified path of the file containing the server's SSL/TLS certificate and private key. The server must have a valid certificate/key file in PEM format in order to use secure sockets. See *Generating an SSL/TLS Certificate and Key File* in this chapter for more information.

The following is an example of a typical SSL/TLS setup viewed from Server Manager:



In Tools Release 9.2.4.3, a new field called ProxyPassword has been added to the Security section in the JDE.ini file of the Enterprise Server. This new field contains the value of the database password and this field must be used only if the Bootstrap User and the Database User are different.



In the previous releases, the Database User and the Bootstrap User were required to have the same password. As of Tools Release 9.2.4.3, you can choose to have different passwords for the Database User and the Bootstrap User. You can also choose to have any combination of long or short passwords for these fields as shown in the following table:

Database User Password	Bootstrap User Password
Long	Long
Short	Short
Long	Short
Short	Long

Additional Setup for TLS Support (Release 9.2.1)

Transport Layer Security (TLS) began with JDK 1.8.3.

```
Enterprise Server/JDK: -Djdk.tls.client.protocols="TLSv1.2"
```

JDENET SSL-Enable Server Authentication (Release 9.2.1)

When JDENET over Secure Sockets Layer (SSL) is enabled, you can enable server authentication. To add server authentication, you need to configure the following two keys to JDENET of both JDE.INI and JAS.INI.

- The numeric key sslServerAuthentication under (JDENET) section specifies whether to enable server certificate authentication or not. It is disabled by default, which means server authentication will not be performed if this key is set to 0 or is missing from JDE.INI or JAS.INI.
- The key sslCAFile under (JDENET) section specifies the location of trusted certificate store/file.

```
[JDENET]

sslServerAuthentication=1

sslCAFile=C:\certstore\CA.pem
```

Creating Certificate Store (Location Specified by sslCAFile)

To create a certificate store in PEM format:

1. Create a blank text file with PEM extension.
2. Gather the server certificates of all the trusted target EnterpriseOne servers.

   From the server certificates, copy the starting and ending content with following two strings into this store:

   ```
   -----BEGIN CERTIFICATE-----

   ….

   -----END CERTIFICATE-----
   ```
3. Place the new file (certificate store) in a location accessible to connecting JDENET entity (EnterpriseOne Server/JAS/FAT Client/Interop Cient) and set the sslCAFile key to the new location.

Enabling TLS v1 for Enterprise Server Prior to 9.2.5

Only TLS v1 is supported on Enterprise Server prior to 9.2.5. Therefore, if you are using Enterprise Server prior to 9.2.5 *and* if you are using JDK/JRE where TLS v1 is set as a disabled algorithm in the `java.security` file, you must remove it from the list of disabled algorithms to enable TLSv1 to communicate with the Enterprise Server, JDENET.

> **Note:** You must enable TLS v1 in the `java.security` file for all the servers in the JD Edwards EnterpriseOne environment as well as all the clients that communicate with the Enterprise Server if they are on the same JDK CPU release, including the Server Manager Console, Server Manager Agent, EnterpriseOne web client, EnterpriseOne development client, EnterpriseOne Server, AIS Server, Business Services Server, and so on.

In the following example, TLS v1 is set as a disabled algorithm in the `java.security` file:

```
jdk.tls.disabledAlgorithms=SSLv3, TLSv1, RC4, DES, MD5withRSA, \ DH keySize < 1024, EC keySize < 224,
3DES_EDE_CBC, anon, NULL, \ include jdk.disabled.namedCurves
```

To enable the TLS v1 algorithm, you must remove it from the disabled algorithms list as shown in the following example:

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, \ DH keySize < 1024, EC keySize < 224, 3DES_EDE_CBC,
anon, NULL, \ include jdk.disabled.namedCurves
```

Configuring the Deployment Server JDE.INI File (Release 9.2.5.1)

Starting with JD Edwards EnterpriseOne Tools Release 9.2.5.1, the Network and Queue Settings (JDENET Configuration) section of the deployment server JDE.INI file contains three settings for SSL or TLS support. These settings are used when the enterprise server connects to the deployment server during a package build from the web client. The deployment server passes the information to the enterprise server on the type of connection to be used. Older enterprise servers that do not support SSL or TLS cannot connect with a deployment server that is enabled with SSL or TLS because of this architecture. Therefore, SSL or TLS support for JDENET requires that the release level of the EnterpriseOne clients matches the release level of the EnterpriseOne servers.

The SSL or TLS settings in the Network and Queue Settings (JDENET Configuration) section of jde.ini are:

- useSSL

  The valid values for this field are `Enable SSL` or `Disable SSL`. If you enable this option, the JDENET messages will be exchanged using secure sockets (SSL or TLS). This setup is done only on the deployment server, but for the setup the enterprise servers accessing the deployment server must be able to process SSL or TLS messages (that is, all the enterprise servers must be running on the same EnterpriseOne ToolsRelease as the deployment server). Starting with EnterpriseOne Tools Release 9.2.5.1, Disable SSL is the default setting.

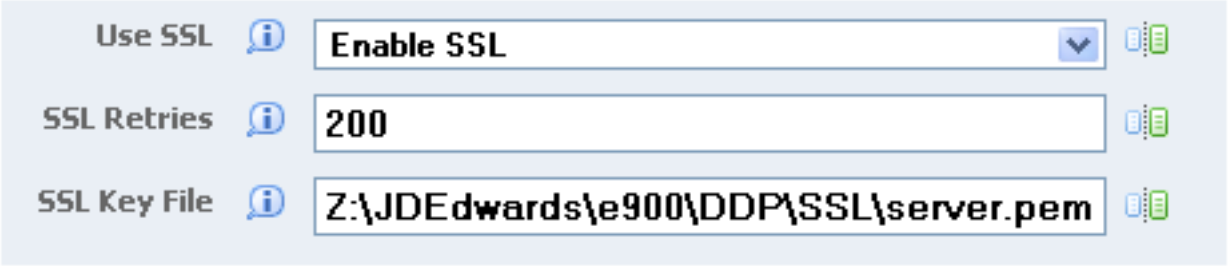
- sslRetries

  This setting specifies the maximum number of times the server or client will attempt to complete an SSL or a TLS handshake. If the handshake is not completed within the retry limit, the SSL or TLS connection fails. The retry limit prevents the server from hanging on an SSL or a TLS connection that may never be established. The default value of 1,000 for this setting should be appropriate for most installations, but may need to be increased to allow for slow clients or high network latency.

- sslKeyFile

  You must set this parameter to the fully qualified path of the file containing the server's SSL/TLS certificate and private key. The server must have a valid certificate/key file in PEM format in order to use secure sockets. See *Generating an SSL/TLS Certificate and Key File* in this chapter for more information.

The following is an example of a typical SSL/TLS setup viewed from Server Manager:



JDENET SSL-Enable Server Authentication (Release 9.2.5.1)

When JDENET over Secure Sockets Layer (SSL) is enabled, you can enable server authentication. To enable server authentication, you need to configure the following two keys to the JDENET section of both the deployment and enterprise servers in the JDE.INI files.

- The numeric key sslServerAuthentication under the [JDENET] section specifies whether to enable server certificate authentication or not. It is disabled by default, which means server authentication will not be performed if this key is set to 0 or is missing from JDE.INI.
- The key sslCAFile under the [JDENET] section specifies the location of the trusted certificate store or file as shown below:

```
[JDENET]

sslServerAuthentication=1

sslCAFile=C:\certstore\CA.pem
```

Creating Certificate Store (Location Specified by sslCAFile)

To create a certificate store in PEM format:

1. Create a blank text file with the PEM extension.
2. Gather the server certificates of all the trusted target EnterpriseOne servers (including the deployment server).
3. From the server certificates, copy the starting and ending content with following two strings into this store:

```
-----BEGIN CERTIFICATE-----

….

-----END CERTIFICATE-----
```

4. Place the new file (certificate store) in a location accessible to the connecting JDENET entity (EnterpriseOne server, JAS, FAT, or Interop client) and set the sslCAFile key to specify the new location.

21 Configuring Transport Layer Security (TLS) for the Database

You must configure TLS (Transport Layer Security) on your database server in order to enable connections from JD Edwards HTML Servers and Development Clients (also called fat clients).

The configuration of TLS on the database server includes these vendor-specific tasks:

- Configure Database for TLS (some databases are pre-configured)
- Certificate and Wallet Creation (both server and client sides)
- Wallet and Certificate Exchange
- Network configuration (both server and client sides)

Enabling TLS on an Oracle Database

Refer to this Oracle document for a description of how to enable TLS on an Oracle database:

https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-secure-sockets-layer-authentication.html

Enabling TLS on a Microsoft SQL Server Database

Refer to these Microsoft documents for a description of how to enable TLS on a SQL Server database:

https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-the-d%5B%E2%80%A6%5Dngine-to-listen-on-multiple-tcp-ports?view=sql-server-ver16

https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver16

https://support.microsoft.com/en-us/topic/kb3135244-tls-1-2-support-for-microsoft-sql-server-e4472ef8-90a9-13c1-e4d8-44aad198cdbe

Enabling TLS on an IBM DB2 Database

Refer to this IBM document for a description of how to enable TLS on an IBM DB2 for IBMi database:

474c456a041f097b8ac56ef57a9616a4591888e2

Refer to this IBM document for a description of how to enable TLS on an IBM DB2 for Linux, UNIX, and Windows database:

https://www.ibm.com/docs/en/db2/11.1?topic=db2-configuring-tls-support-instance

22 Configuring SSL for EnterpriseOne Servers

Understanding SSL for EnterpriseOne Servers

Secure Sockets Layer (SSL) is a cryptographic protocol that enables secure communication between applications across a network. SSL requires certificates signed by a certificate authority to establish secure communication between servers.

Configure SSL for all EnterpriseOne servers that run on an application server, which include:

- EnterpriseOne HTML Server
- EnterpriseOne Transaction Server
- Oracle BI Publisher Server
- EnterpriseOne Application Interface Services (AIS) Server
- EnterpriseOne Orchestrator Studio Server.

  The Orchestrator Studio can be deployed only on an Oracle WebLogic Server with ADF runtime. If the other servers in this list are deployed on Websphere, you will need to exchange certificates between the different application server types.
- Oracle Application Development Framework (ADF) Server
- EnterpriseOne Business Services Server

In addition, you must configure SSL for the EnterpriseOne Enterprise Server, which does not run on an application server. An SSL configuration on the Enterprise Server provides secure communication between this server and the AIS Server.

For both Oracle WebLogic Server and IBM WebSphere Application Server, the SSL implementation should support the latest version of the Transport Layer Security (TLS) protocol. SSL in Oracle WebLogic Server and IBM WebSphere Application Server is an implementation of the SSL and TLS specifications.

Note: For general information about an SSL implementation for your application server type, refer to these resources:

- *"Overview of Configuring SSL in WebLogic Server" in the Fusion Middleware Administering Security for Oracle WebLogic Server* .
- For IBM WebSphere Application Server, refer to "Secure Communications Using Secure Sockets Layer," located here: `https://www.ibm.com/support/knowledgecenter/en/SSEQTP_8.5.5/com.ibm.websphere.base.iseries.doc/ae/csec_sslsecurecom.html`

Considerations for On-Premise and One-Click Provisioning Environments

On-premise EnterpriseOne servers deployed on Oracle WebLogic Server come with a demo certificate, but SSL is not enabled by default.

For JD Edwards One-Click Provisioning for Oracle Cloud, SSL is enabled on all servers using a self-signed certificate.

For a production environment, Oracle strongly recommends enabling SSL for all servers using a certificate from a reputable certificate authority.

Configuring SSL for EnterpriseOne Servers on Oracle WebLogic Server

This section contains the following topics:

- *Obtaining and Installing CA Certificates on WebLogic Server*
- *Enabling TLS on Oracle WebLogic Server*
- *Configuring SSL on Oracle HTTP Server*
- *Disabling Non-SSL Ports*
- *Updating Server Configuration Settings to Use the HTTPS Protocol*

Obtaining and Installing CA Certificates on WebLogic Server

On the physical machine with an Oracle WebLogic Server running an EnterpriseOne server, create a keystore and configure it with a certificate. If you have multiple EnterpriseOne servers installed within the same domain, you need only a single certificate for the keystore.

The following steps outline the process to create a keystore and generate a Certificate Signing Request (CSR), which is described in detail in the *"Configuring Keystores: Main Steps" in the Oracle Fusion Middleware Administering Security for Oracle WebLogic Server 12.2.1.2.0 Guide* . After performing these tasks, use the HTTPS protocol to verify access to each SSL-enabled server.

1. Create the keystore that will hold the server identity certificate.
2. Create a Certificate Signing Request (CSR), and submit it to a Certificate Authority.

   For a production environment, Oracle strongly recommends obtaining a certificate from a reputable certificate authority
3. Import the identity and trust certificates returned by the Certificate Authority.
4. Configure the trust and identity keystores with Oracle WebLogic Server.

Enabling TLS on Oracle WebLogic Server

Enable TLSv1.2 on each Oracle WebLogic Server on which an EnterpriseOne server or Server Manager Console is installed. To do so, on the Server Start tab, enter the following parameter in the Arguments field:

```
-Dweblogic.security.SSL.minimumProtocolVersion= TLSv1.2
```

For more information about the support of TLS in Oracle WebLogic Server, see *"Specifying the SSL Protocol Version" in the Oracle Fusion Middleware Administering Security for Oracle WebLogic Server 12.2.1.2.0 Guide* .

Configuring SSL on Oracle HTTP Server

If you use Oracle HTTP Server to direct web traffic to your EnterpriseOne system, you should configure it with SSL. For Oracle HTTP Server, instead of creating a keystore, you create an Oracle wallet with the -auto_login_only option for storing the certificate. See *"Managing Keystores, Wallets, and Certificates" in the Administering Oracle Fusion Middleware 12.2.1 Guide* .

If any of the EnterpriseOne servers are not on the same physical machine as Oracle HTTP Server, you must exchange certificates between the machine with the EnterpriseOne server and the Oracle HTTP Server machine.

Disabling Non-SSL Ports

After you set up SSL for each managed server, based on your network configuration, you may want to disable the non-SSL port of each managed server. To do so:

1. On the WebLogic Administrator Console, clear or uncheck the Listen Port.
2. Because the http protocol is no longer available, add the following Java argument to the Server Start tab:

```
-Dweblogic.DefaultProtocol= t3s
```

Updating Server Configuration Settings to Use the HTTPS Protocol

After configuring SSL for managed EnterpriseOne servers, in Server Manager, update each managed server's End Point Protocol setting to use the HTTPS protocol.

Configuring SSL for EnterpriseOne Servers on IBM WebSphere Application Server

This section contains the following topics:

- *Obtaining and Installing CA Certificates on IBM WebSphere Application Server*
- *Configuring SSL on IBM HTTP Server*
- *Disabling Non-SSL Ports*
- *Updating Server Configuration Settings to Use the HTTPS Protocol*

Obtaining and Installing CA Certificates on IBM WebSphere Application Server

On the physical machine with an IBM WebSphere Application Server running an EnterpriseOne server, create a keystore and configure it with a certificate. If you have multiple EnterpriseOne servers installed within the same domain, you only need a single certificate for the keystore.

For IBM WebSphere Application Server, see "Secure communications using Secure Sockets Layer (SSL)" located here:

https://www.ibm.com/support/knowledgecenter/SSEQTP_9.0.0/com.ibm.websphere.base.doc/ae/csec_sslsecurecom.html

Configuring SSL on IBM HTTP Server

If you use IBM HTTP server to direct web traffic to your EnterpriseOne system, you should configure it with SSL.

If any of the EnterpriseOne servers are not on the same physical machine as IBM HTTP server, you must exchange certificates between the machine with the EnterpriseOne server and the IBM HTTP server machine.

Refer to the following instructions on the IBM Knowledge Center on how to configure IBM HTTP server SSL support:

http://www-01.ibm.com/support/docview.wss?uid=swg21179559

Disabling Non-SSL Ports

After you set up SSL for each managed server, based on your network configuration, you may want to disable the non-SSL port of each managed server. To do so:

1. Log in to IBM WebSphere Integrated Solution Console.
2. Select **Environment Hosts**, **Virtual Hosts**, **default_host**, **Host Aliases**.
3. Remove the non-SSL port.
4. Save the changes.

Updating Server Configuration Settings to Use the HTTPS Protocol

After configuring SSL for managed EnterpriseOne servers, in Server Manager, update each managed server's End Point Protocol setting to use the HTTPS protocol.

Configuring SSL Between the EnterpriseOne Enterprise Server and AIS Server

The Enterprise Server provides user authentication for requests sent to the AIS Server. Starting with EnterpriseOne Tools 9.2.3, it is also used to execute calls to orchestrations and notifications on the AIS Server. Enable SSL on the Enterprise Server to provide secure communication between these servers. For the Enterprise Server, SSL is enabled through the Server Manager agent running on the Enterprise Server.

This section contains the following topics:

- *Enabling SSL on the Enterprise Server on IBM i*
- *Enabling SSL on the Enterprise Server on UNIX and Microsoft Windows*

Enabling SSL on the Enterprise Server on IBM i

On IBM i, use IBM i Digital Certificate Manager to enable SSL on the Enterprise Server. For details, see "How to Import a CA Certificate into Digital Certificate Manager" located here:

http://www-01.ibm.com/support/docview.wss?uid=nas8N1012543

These instructions assume that the *SYSTEM store has already been created and that the user knows the password for that store. If you have not created a *SYSTEM store, see "How to Create the *SYSTEM Store in DCM" located here:

https://www-01.ibm.com/support/docview.wss?uid=nas8N1010320

The preceding instructions describe how to import one certificate at a time. If you import more than one certificate, you need to comment out (#) all the lines in first certificate or delete the lines in the first certificate, and then repeat the process for the remaining certificates in the file.

Enabling SSL on the Enterprise Server on UNIX and Microsoft Windows

On UNIX and Windows, the HTTPS SSL communication between the Enterprise Server and AIS Server depends on having a valid cacert.pem file in your system/bin32 directory that contains an up-to-date set of root certificates from the SSL certificate issuing authorities. Starting with EnterpriseOne Tools 9.2.3, the release is delivered with a cacert.pem that was current near the time of the release and in most cases, should work with no additional configuration required. However, you may need to update this file from time to time. You can download a current copy from the "libcurl" open-source website at: ***https://curl.haxx.se/docs/caextract.html***

The root certificates are typically updated every 4-6 months. The cacert.pem file is a text file. which contains the date of the last update, so you can check the date to determine if there has been an update.

In most cases, after the SSL certificate is registered on the machine where the web application server is hosting the AIS Server, and communication between this machine and the Enterprise Server has been configured successfully, you will not need to update the root certificates in cacert.pem again. However, you will need to update the root certificates when the current AIS Server SSL certificate expires and a new AIS Server SSL certificate is needed.

Exchanging Certificates Between EnterpriseOne Servers

An EnterpriseOne system typically includes an architecture with multiple EnterpriseOne servers installed on different machines, for example an EnterpriseOne HTML Server on one machine and an EnterpriseOne AIS Server on a different machine. In this case, to establish SSL between servers on different machines, you need to import the certificate of each machine into the other machine's keystore.

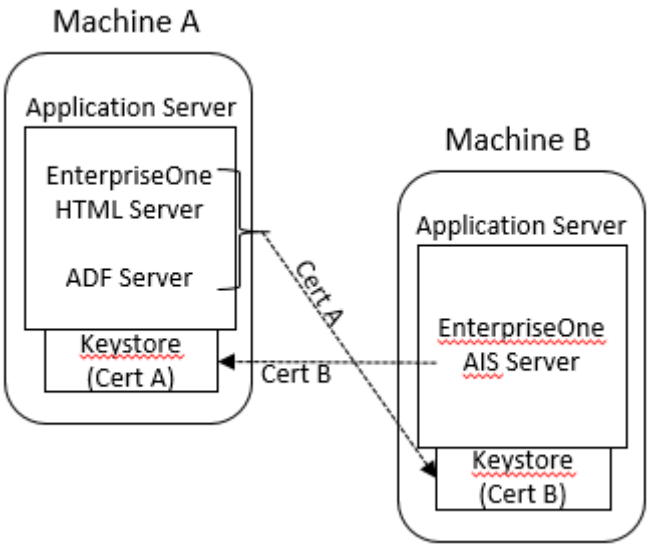
> **Note:** To avoid having to determine which servers are in direct communication, you can simply import the certificates from each machine's keystore into the keystore of all server machines in your EnterpriseOne configuration. This will eliminate any gaps in your SSL implementation.

For detailed steps on how to import a certificate into a keystore on Oracle WebLogic Server, see *"Importing Certificates into the Trust and Identity Stores" in the Oracle Fusion Middleware Administering Security for Oracle WebLogic Server Guide* .

For detailed steps on how to import a certificate into a keystore on IBM WebSphere Application Server, refer to the following site:

https://www.ibm.com/support/knowledgecenter/en/SSEQTP_8.5.5/com.ibm.websphere.base.iseries.doc/ae/tsec_sslconfiguration.html

#unique_489/unique_489_Connect_42_BABHGAEF shows an example of certificates exchanged between two machines. Machine A has an application server with two managed servers: an EnterpriseOne HTML Server and an Oracle ADF Server. Machine B has a application server running the EnterpriseOne AIS Server. To establish SSL communication between these servers, a single certificate (Cert A) for the managed servers on Machine A was imported into the keystore on Machine B. The certificate (Cert B) for the managed server on Machine B was imported into the keystore on Machine A.



Configuring SSL for Server Manager Console and Server Manager Agents

Enable SSL for the Server Manager Console and Server Manager agents.

To enable SSL for the Server Manager Console, you must obtain and install CA Certificates on the Oracle WebLogic Server machine where Server Manager Console is installed. See *Obtaining and Installing CA Certificates on WebLogic Server* in this chapter for details.

To enable SSL for Server Manager agents, import the Server Manager Console certificate into each Server Manager Agent Truststore/Keystore:

1. Export the Server Manager Console certificate to a file using these steps:
   a. From the browser, click the lock icon on the left hand side of the URL of the HTTPS/SSL based Server Manager Console URL.
   b. Click **Certificate Information**.
   c. Go to the Details tab and select the **Copy to File** option.
   d. Click **Next**.
   e. Select **DER encoded binary X.509 (.CER) format**.
   f. Click **Next**.
   g. Enter file information.
   h. Click **Next**.
   i. Click **Finish**.

      If configured correctly, an "Export is Successful" message appears.
   j. You can view the certificate in the path given in the above step.
2. Import the Certificate into the Truststore/Keystore of each of the Server Manager Agents (cacerts file of `x:\jde_home_1\SCFHA\jdk\jre\lib\security\cacerts file`).

   > **CAUTION:** Before performing the import, back up the cacerts file located at `x:\jde_home_1\SCFHA\jdk\jre\lib\security\<cacertsfile>`.

3. Import the Certificate using the keytool command, for example:

   ```
   >keytool -import -alias <your_alias> -file <cert_file> -keystore <keystore location>
   ```

   This is the syntax to import the Certificate file on a Windows platform. Use the appropriate command to perform this step on Linux/UNIX/AS400 platforms and also for Server Manager Agents installed on these platforms.

   When prompted for whether you trust the Certificate, answer **Yes**.
4. If the default password for cacerts file has been changed, then use the appropriate password.
5. After this step, restart the Server Manager Agent.

   Perform this step on each of the Server Manager Agent machines. Without this step, the Server Manager Agent may not be able to communicate with the Server Manager Console.

6. Sign in to Server Manager Console to verify the connections.

   This completes the configuration required for running the Server Manager Console on Oracle WebLogic Server with HTTPS/SSL enabled and completes the importing of the certificate on the Server Manager Agents.

Hostname Mismatch Errors

If the hostname in the certificate generated by Oracle WebLogic Server does not exactly match the Fully Qualified Hostname of the Server Manager Console machine, then you will see the type of errors listed below in the Server Manager Agent stderr.log/e1agent.logs.

In this case, you need to create a valid Self Signed Certificate using the keytool utility and import the certificate into the WebLogic Custom Truststore and Custom Keystore. Also, you will need to configure WebLogic to use the Custom Truststore and Custom Keystore. This Self Signed Certificate will also need to be imported in the cacerts file of the Server Manager Agents.

```
javax.net.ssl.SSLException: hostname in certificate didn't match:
<10.1.1.1> != <server.example.com> at
org.apache.http.conn.ssl.AbstractVerifier.verify(AbstractVerifier.java:227) at
org.apache.http.conn.ssl.BrowserCompatHostnameVerifier.verify(BrowserCompatHostna
meVerifier.java:54) at
org.apache.http.conn.ssl.AbstractVerifier.verify(AbstractVerifier.java:147) at
 org.apache.http.conn.ssl.AbstractVerifier.verify(AbstractVerifier.java:128) at
org.apache.http.conn.ssl.SSLSocketFactory.connectSocket(SSLSocketFactory.java:437
) at
org.apache.http.impl.conn.DefaultClientConnectionOperator.openConnection(DefaultC
lientConnectionOperator.java:180) at
org.apache.http.impl.conn.ManagedClientConnectionImpl.open(ManagedClientConnectio
nImpl.java:294) at
org.apache.http.impl.client.DefaultRequestDirector.tryConnect(DefaultRequestDirec
tor.java:643) at
org.apache.http.impl.client.DefaultRequestDirector.execute(DefaultRequestDirector
.java:479) at
org.apache.http.impl.client.AbstractHttpClient.execute(AbstractHttpClient.java:90
6) at
org.apache.http.impl.client.AbstractHttpClient.execute(AbstractHttpClient.java:80
5) at
org.apache.http.impl.client.AbstractHttpClient.execute(AbstractHttpClient.java:78
4) at
com.jdedwards.mgmt.agent.UserPasswordCallBack._getUserCredentials(UserPasswordCal
lBack.java:40) at
com.jdedwards.mgmt.agent.UserPasswordCallBack.<init>(UserPasswordCallBack.java:31
) at
com.jdedwards.mgmt.agent.E1Agent$ManagementServerDaemonThread.run(E1Agent.java:22
59) at java.lang.Thread.run(Thread.java:722)
```

Disabling Weak Cipher Suites

Weak cipher suites are vulnerable to cyber attacks and therefore can expose a security gap. This section describes two different methods for handling weak cipher suites:

- *Explicitly Configuring Ciphers in Oracle WebLogic Server*

  This is a one-time, but tedious and lengthy process.

- *Disabling Weak Cipher Suites Globally Through Java*
  This method is easier, but must be repeated each time you receive a Java update.

Regardless of the method you choose, after disabling weak cipher suites, confirm the cipher suite has been disabled as described in *Verifying Weak Cipher Suites Have Been Disabled*.

> **Note:** Refer to Document 1067411.1 on My Oracle Support (`https:\\support.oracle.com`) for information about anonymous and weak SSL cipher suites in Oracle WebLogic Server. This document includes considerations and guidelines for Oracle Fusion Middleware products.

Explicitly Configuring Ciphers in Oracle WebLogic Server

You may need to explicitly configure a cipher or cipher list depending on your version, business decisions, and other requirements. You should explicitly disable ciphers that support clear text communication. The server allows clear text communication either because strong cipher suites are not specified or null cipher suites are specified. To prevent clear text communications, avoid ciphers such as TLS_RSA_WITH_NULL_MD5 and TLS_RSA_WITH_NULL_SHA, as these have 0 Symmetric Key Strength. Refer to the Oracle Documentation specific to your version of Oracle WebLogic Server for which ciphers are supported.

On older 10.3 versions that do not support a newer JDK update, if no cipher suite is specifically mentioned in the config.xml file, then the cipher suites that allow clear text communication may be enabled on the server by default. To disable these clear text cipher suites, set the following as JAVA_OPTIONS during startup:

```
-Dweblogic.security.disableNullCipher=true
-Dweblogic.security.SSL.allowUnencryptedNullCipher=false
```

For all versions, the domain's config.xml file may also be configured for the cipher suite that you want to use. To specify a cipher suite, add the attributes below and specify any cipher suites as needed (and as supported by both sides of the communication to establish a handshake). For example:

- In WebLogic Server 12c, you may add the `<ciphersuite>` tag in the config.xml with ciphers you wish to use: Ensure `<ciphersuite>` is added before the `<listen-port>` as below for admin and managed servers:
  ```
  <ssl>
                  <name>AdminServer</name>
                  <enabled>true</enabled>
                  <ciphersuite>enter_a_cipher_of_your_choice_here</ciphersuite>
                  <ciphersuite>enter_another_optional_cipher_of_your_choice_here</
  ciphersuite>
                  <listen-port>7002</listen-port>
                  <login-timeout-millis>25000</login-timeout-millis>
                  ...
  ```
  You may have the Admin Server with a "false" setting because of this documentation. You edit it the same way, usually only because something is detecting an undesirable cipher.

Node Manager

To allow the Node Manager to use stronger ciphers, the WebLogic Server version must be at least 10.3.6.0.10, 12.1.2.0.4 or 12.1.3.0.3 (which are PSU versions delivered early 2015; see Document 1470197.1 on My Oracle Support for the latest). The nodemanager.properties may be used to customize ciphers, but will not work correctly with Node Manager unless the PSUs are applied. After the PSU is applied and JDK updated, it is recommended to allow the default processing to take place.

Use caution if setting this manually. You need to discover all supported ciphers with which the Node Manager needs to perform a handshake, including other internal middleware processes. By default, it is not required to update the ciphers for null, under 128-bit, weak, or vulnerabilities if you are updating the JDK and applying PSUs. A manual configuration is not recommended unless you have a strict business requirement to use a specific cipher suite.

1. Open nodemanager.properties file.
2. Access the following parameter and enter a cipher:

   ```
   CipherSuite=enter_a_cipher_of_your_choice_here
   ```
3. Locate your startnodemanager script file called startNodeManager.sh or startNodemanager.cmd, which you can usually find in the `WLS_HOME/server/bin` directory.
4. Add the flag for your JAVA_OPTIONS to your startnodemanger script file:

   ```
   -Dweblogic.security.SSL.Ciphersuites=enter_a_cipher_of_your_choice_here
   ```

Note:

- The cipher you choose must begin with SSL_ (even if using TLS) and must be compatible with other entities requiring a connection (such as other Oracle Fusion Middleware tools and components)
- You can only configure a cipher supported by the JDK you have installed (and certified with WebLogic Server):

  ```
  https://docs.oracle.com/javase/8/docs/technotes/guides/security/SunProviders.html#SunJSSEProvider
  ```
- Check other JAVA_OPTION settings you may have configured earlier which could conflict with this. This will need to be compatible with the WebLogic Servers being started by node manager.

See Document 2286346.1 "Securing Node Manager Port with High Level SSL Ciphers and Disabling Undesired Algorithms" on My Oracle Support (*https:\\support.oracle.com*).

Disabling Weak Cipher Suites Globally Through Java

You can disable weak cipher suites globally through Java. The JAVAHOME directory has a security file in which you can disable weak cipher suites. Any software, such as Oracle WebLogic Server, that uses this installation of Java will then have them disabled.

Note: If you have the latest JDK, this is done automatically.

To disable weak cipher suites such as DES and 3DES globally through Java:

1. At a command prompt, access the java.security file:

   ```
   JAVA_HOME/jre/lib/security/java.security
   ```
2. Open the java.security file and locate the following parameter:

   ```
   jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 768
   ```
3. In this line, after `=SSLv3`, add `DES` and `DESede` so that the line looks like this:

```
jdk.tls.disabledAlgorithms=SSLv3, DES, DESede, RC4, MD5withRSA, DH keySize < 768
```

4. Verify that weak cipher suites have been disabled. See *Verifying Weak Cipher Suites Have Been Disabled*.

Verifying Weak Cipher Suites Have Been Disabled

You can use openssl to test if a cipher is enabled or disabled. At a command prompt, enter the following commands.

```
$ openssl s_client -host <hostname> -port <port> -cipher 3DES

$ openssl s_client -host <hostname> -port <port> -cipher DES
```

Each command should return a failure message that looks similar to the following message:

```
CONNECTED(00000003)
140209911707464:error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake
 failure:s23_clnt.c:672:
```

23 Working with Transport Layer Security (Release 9.2.7.3)

Overview

The following JD Edwards EnterpriseOne systems can use Transport Layer Security (TLS) to communicate with the Database server.

- Enterprise Server
- Deployment Server
- Development Client

To enable the client communication with Database server using TLS, database server CA certificates must be imported to these JD Edwards EnterpriseOne systems.

The below sections list the steps to import certificates and configure the database client to facilitate the TLS communication for the following supported databases.

Oracle

Connectivity to an Oracle database server is provided by Oracle database clients, which must be already installed.

The orapki utility is available with the database client installation. You must use this utility to create a wallet and import the database server CA certificate file to this wallet. The utility is typically located in the Oracle client installation path. For example:

```
<ORACLE_CLIENT_HOME>/bin/orapki
```

Creating a New Auto-Login Wallet to Store the Certificates

1. Use the following command to create a directory for the wallet that you will create:

   ```
   mkdir -p <path>/wallet
   ```

   Example:

   ```
   mkdir -p /u01/app/oracle/wallet
   ```

2. Use the following command to create a new auto-login wallet:

   ```
   orapki wallet create -wallet <path>/wallet -pwd <password> -auto_login_local
   ```

   Example:

   ```
   orapki wallet create -wallet "/u01/app/oracle/wallet" -pwd WalletPasswd123 -auto_login_local
   ```

Importing CA-Signed Certificates from the Database Server

Note: The CA-signed certificates for your database server must be provided to you by your system administrator.

Use the following commands to load CA-signed certificates for your Oracle database client wallet:

Root Certificate

```
orapki wallet add -wallet <wallet_path> -pwd WalletPasswd123 -trusted_cert -cert rootca.pem
```

Example:

```
orapki wallet add -wallet "/u01/app/oracle/wallet" -pwd WalletPasswd123 -trusted_cert -cert c:\rootca.pem
```

Intermediate Certificate

```
orapki wallet add -wallet <wallet_path> -pwd WalletPasswd123 -trusted_cert -cert interca.pem
```

Example:

```
orapki wallet add -wallet "/u01/app/oracle/wallet" -pwd WalletPasswd123 -trusted_cert -cert c:\interca.pem
```

Configuring the tnsnames.ora and listener.ora Files

Update the `<wallet location>` in the `listener.ora` file of the Oracle Database client as shown below:

```
 WALLET_LOCATION =
 (SOURCE =
 (METHOD = FILE)
 (METHOD_DATA =
 (DIRECTORY = <wallet_location>
)
)
SQLNET.AUTHENTICATION_SERVICES = (TCPS,NTS)
 SSL_CLIENT_AUTHENTICATION = FALSE
 SSL_CIPHER_SUITES = (SSL_RSA_WITH_AES_256_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA)
```

Update the `Protocol` and `Port` value in the `tnsnames.ora` file of the Oracle Database client.

```
JDEORCL=
 (DESCRIPTION=
 (ADDRESS=
 (PROTOCOL=TCPS)
 (HOST=<DB_server_host_name>)
 (PORT=1522)
)
 (CONNECT_DATA=
 (SERVER=dedicated)
 (SERVICE_NAME=JDEORCL)
)
)
```

Microsoft SQL Server

Connectivity to a Microsoft SQL Server database server is provided by SQL Server clients, which must be already installed.

Importing CA-Signed Certificates from the Database Server

You must obtain the Database Server, Root and Intermediate CA certificates. These certificates are typically named with basic naming convention:

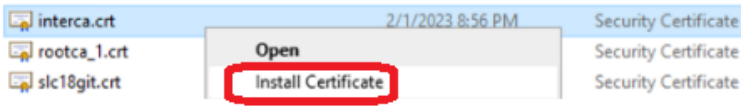
- `<server_cert>.crt`
- `rootca.crt`
- `interca.crt`

Importing CA-Signed Certificates

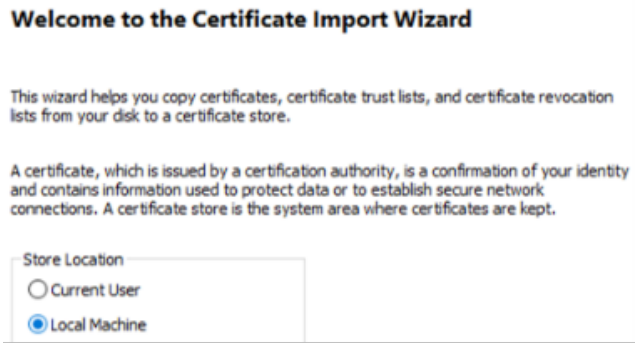
In Windows Explorer on the SQL Server database client machine, locate the database server CA certificates which you obtained.

Follow the below steps to import each of the database server certificates into Trusted Root Certificates authorities of the Client machine:

1. Right click on a CA certificate.
2. Click on **Install Certificate**.



3. On Welcome to the Certificate Import Wizard, click the radio button for Local Machine and click the **Next** button to continue.



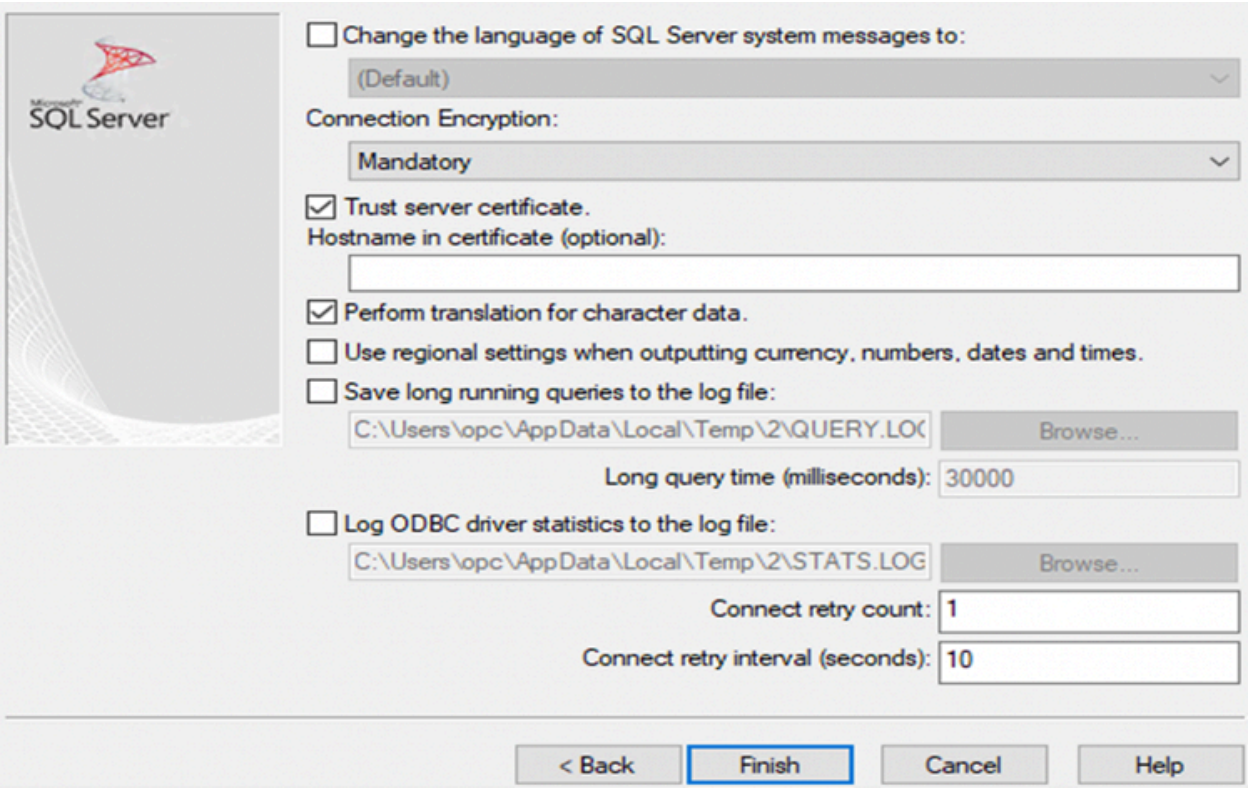
4. When you are prompted for the Certificate Store, choose **Place all certificates in the following store**.
5. Select the **Trusted Root Certification Authorities store**.
6. Complete the remaining steps of the wizard and click the **Finish** button.

Configuring the ODBC Driver for Encryption

You must configure the SQL Server ODBC to enable encryption.

For example, with SQL Server ODBC Driver, follow the below settings:

- Connection Encryption is set to Mandatory.
- Trust server certificate checkbox is selected.
- The Hostname in certificate field must match the hostname in the database server certificate.



IBM DB2 UDB

Ensure that the GSkit level corresponds to the DB2 client version as defined in the IBM Support:

GSKit Versions Shipped with DB2

Creating a New Keystore Database and Stash to Store the Certificates

Use the following command to create a new Keystore database and Stash:

```
gsk8capicmd_64 -keydb -create -type cms -db <keystore_database_path>/<keystore_database_name> -pw <
keystore_password > -stash
```

Example:

```
gsk8capicmd_64 -keydb -create -type cms -db /slot/ems4974/appmgr/ssl_client/slc18gjx.kdb -pw Tools123 -stash
```

Importing CA-signed Database Server Certificates

Note: The CA-signed certificates for your database server must be provided to you by your system administrator.

Use the following commands to load CA-signed certificates for your IBM UDB database client wallet:

Server Certificate

```
gsk8capicmd_64 -cert -add -db <keystore_database_path>/<keystore_database_name> -pw <keystore_password> -file
<server_certificate_location> -label <certificate_label>
```

Example:

```
gsk8capicmd_64 -cert -add -db "mydbclient.kdb" -pw "myClientPassw0rdpw0" -file C:\Users\sagautha\Desktop
\aix_reg_certificates\slc18git.pem -label slc18git_SSL
```

Root Certificate

```
gsk8capicmd_64 -cert -add -db <keystore_database_path>/<keystore_database_name> -pw <keystore_password> -file
<root_certificate_location> -label <certificate_label>
```

Example:

```
gsk8capicmd_64 -cert -add -db "mydbclient.kdb" -pw "myClientPassw0rdpw0" -file C:\Users\sagautha\Desktop
\aix_reg_certificates\rootca_1.pem -label rootca_SSL
```

Intermediate Certificate

```
gsk8capicmd_64 -cert -add -db <keystore_database_path>/<keystore_database_name> -pw <keystore_password> -file
<inter_certificate_location> -label <certificate_label>
```

Example:

```
gsk8capicmd_64 -cert -add -db "mydbclient.kdb" -pw "myClientPassw0rdpw0" -file C:\Users\sagautha\Desktop
\aix_reg_certificates\interca.pem -label interca_SSL
```

Updating the Default Values for Keystore and Stash

Use the following command to update the default values for keystore and stash:

```
db2 update dbm cfg using SSL_CLNT_KEYDB C:\Users\<user>\mydbclient.kdb SSL_CLNT_STASH C:\Users\<user>
\mydbclient.sth
```

Running the Catalog Command for the Database SSL Port

Use the following catalog command to run the catalog command for the database SSL port:

```
db2 catalog tcpip node slc18git remote <machine> server 50001 security SSL
```

Enabling TLS on the Development Client

To enable communication between Development Client and Database Server using TLS, update following configuration in the JDE.ini file of the Development Client.

```
[DB SYSTEM SETTINGS]

ServerPort=<database TLS port>
```

Note: The port value varies depending on your database server. It is initially set during installation of EnterpriseOne. You must update this value to use specific TLS port of the database server. Typically, Oracle and IBM DB2 UDB has different ports for both secured and unsecured connections.

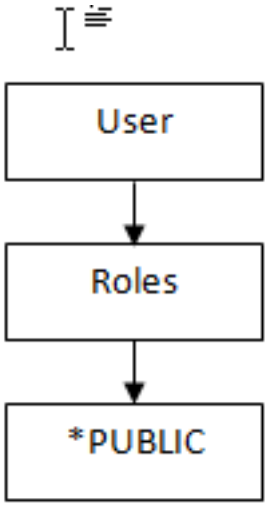
24 Understanding Authorization Security

JD Edwards EnterpriseOne Authorization Model

JD Edwards EnterpriseOne authorization security enables a security administrator to control security for individual users and for groups of users. Setting up security correctly ensures that users in the system have permission to perform only those actions that are essential to the completion of their jobs.

The JD Edwards EnterpriseOne authorization security model is not secured by default. You should explicitly lock down all users by setting up different types of EnterpriseOne security for *PUBLIC, and then set up inclusive security to grant rights to roles.

EnterpriseOne applies authorization security in the following sequence for the signed-in user:



When a user attempts to access an application or perform an action, EnterpriseOne checks security for that particular user ID. If security exists for that user ID, the software displays a message indicating that the user cannot proceed.

If the user ID has no security, the software checks role profiles (if that user is part of a specific role), and then *PUBLIC for security. If no security is established at any of these levels, the software allows the user to continue.

EnterpriseOne also provides software license security through protection codes, and it requires user validation at sign-in and when accessing new data sources.

Users, Roles, and *PUBLIC

The EnterpriseOne security administrator can set up security for:

- A particular user

  This option controls security by specific EnterpriseOne user ID.
- A user role

  This option controls security by role, which enables you to group users based on similar job requirements. An example is putting all of the accounts payable clerks in one role, such as Accounts Payable (AP).
- All users

  This option controls security for all users who are designated by ID type ***PUBLIC** in the User or Role field. The designation ***PUBLIC** is a special ID within EnterpriseOne that automatically includes all of the users within it. You can use this ID to apply security even if you do not have a specific record set up for it in user profiles.

Object-Level Security

EnterpriseOne authorization security is at the object level. This level means that you can secure specific objects within EnterpriseOne, which provides flexibility and integrity for your security. For example, you can secure a user from a specific form and then, no matter how the user tries to access the form (using a menu or any application that calls that form), the software prevents access to the form. The software simplifies the process of setting up security by enabling you to set security for hundreds of objects at one time by securing all objects on a specific menu or by securing all objects under a specific system code.

The Security Workbench application (P00950) enables you to secure EnterpriseOne objects, such as applications, forms, rows, tabs, and so on. It stores all objects security records in the F00950 table.

> **Note:** Only the objects are secured; the software does not support menu or system code security. Object security provides a higher level of integrity. For example, if you secured a specific menu to prevent users from accessing the applications on that menu, the users might still be able to access those applications through another menu or another application that accesses the applications that you wanted to secure.

Object Level Security Types

At specific object levels, you can set these levels of security, alone or in any combination, for users and groups of users assigned to a particular role:

Application security

Secures users from running or installing, or both, a particular application, an application version, or a form within an application or application version. You cannot define Application security at the subform level. Application security also applies to EnterpriseOne mobile applications.

Action security

Secures users from performing a particular action, such as adding, deleting, revising, inquiring, or copying a record. You define Action security at the application, version, and form level. You cannot define Action security at the subform level.

Row security

Secures users from accessing a particular range or list of records in any table. For example, if you secure a user from accessing data about business units 1 through 10, the user cannot view the records that pertain to those business units.

Column security

Secures users from viewing a particular field or changing a value for a particular field in an application or application version. This item can be a database or non-database field that is defined in the data dictionary, such as the work/calculated fields. For example, if you secure a user from viewing the Salary field on the Employee Master application, the Salary field does not appear on the form when the user accesses that application.

Processing option security

Secures users from viewing or changing the values of processing options, or from prompting for versions and prompting for values for specific applications or application versions. For example, if you secure a user from changing the processing options for Address Book Revisions, the user could still view the processing options (if you did not secure the user from prompting for values), but would not be able to change any of the values.

If you secure a user from prompting for versions, the user would not be able to see the versions for a specific application, so the user would not be able to select a different version of an application from the version that the administrator assigned.

Tab security

Secures users from viewing or changing fields in a tab or tabs on a given form. You define Tab security at the application, version, and form level. You cannot define Tab security at the subform level.

Hyper exit security

Secures users from menu bar exits on JD Edwards EnterpriseOne forms. These exits call applications and allow users to manipulate data. Exit security also restricts use of the same menu options.

Exclusive application security

Overrides row security that is set for an application. When you set exclusive application security for a user, the system overrides row security for every table that is accessed by the application that is specified. All other security still applies.

External calls security

Secures users from accessing standalone executables that exist external to JD Edwards EnterpriseOne. These external executables, which might include design tools, system monitors, and debugging tools, are specific to JD Edwards EnterpriseOne.

Solution Explorer security

Secures users from performing and viewing certain features within Solution Explorer, such as Menu Filtering and Fast Path.

Miscellaneous security

Provides additional security options to prevent users from running reports that update EnterpriseOne database tables. You can also use Miscellaneous security to configure different levels of access to workflows.

Data Browser security

Controls access to the Data Browser application.

Push button, image, and link security

Controls whether users can user or view push button, link, and image controls.

Media object security

Controls whether users can add, change, delete, or view media objects within interactive applications, forms, or application versions.

Text Block and Chart Control security

Controls whether users can use or only view text block and chart controls.

Application query security

Prevents users from performing searches if they have not entered search criteria in the form filter fields or QBE fields.

Published business service security

Controls access to published business services. For published business services, EnterpriseOne uses a "secure by default" security model which means that users cannot access a published business service unless a security record exists that authorizes access. For all other objects in JD Edwards EnterpriseOne, access is granted unless otherwise secured or restricted.

User defined object security

EnterpriseOne enables you to set up security for objects created by end users, otherwise referred to as user defined objects (UDO). For instructions on how to set up UDO security, see *Managing Security for User Defined Objects*.

Authorization Security for Business Units

EnterpriseOne business unit security provides the ability to filter data by business unit for UDCs and for transaction tables. For UDCs, you create subgroups of values that can be shared among various business units or might be unique to one particular business unit. This is referred to as UDC sharing. For transaction tables, business unit security enables you to limit the transaction records that a user can access based on business unit. This is called transaction security.

With UDC sharing, EnterpriseOne provides the ability to control or regulate how organizational data among different business units is shared.

Transaction security enables you to determine the transaction records a user can view. Transaction security ensures that users can only access and modify transaction data for the business unit to which they are associated.

You should set up business unit security when users are allowed to access data only for their business unit.

See *Setting Up Business Unit Security* in this guide for more information on business unit security.

Authorization Security for Notifications

Notifications send information from your JD Edwards system to your subscribers. Therefore, you must be aware of JD Edwards security so that the subscribers get the information they need and do not get the information from which they are secured. In general, the security of your notifications will depend on two things:

- The resources or objects that you include in your notification, such as Watchlists or orchestrations, and the resources that they, in turn, invoke.
- The user ID under which the notification runs.

See *Managing Notifications and UDO Security* in the *JD Edwards EnterpriseOne Tools Notifications Guide* for more information.

Cached Security Information

When changes to security are made using the Security Workbench application (P00950), the changes are not immediately recognized in any environment because the records in the system data source are cached. For security changes to be enabled, the cache must be cleared.

Clearing the Cache on a Workstation Client

If system administrators make changes to the P00950 table, the changes are not immediately realized on workstations that are logged on to the system while security revisions are being made. To enable security changes, you clear the workstation's memory cache by signing off and signing back on to the workstation.

Clearing the Cache on a Web Client Using Server Manager

To clear the cache on a web client for JD Edwards EnterpriseOne Tools 8.97 and later releases, you use Server Manager.

Use these steps to clear the cache using Server Manager:

1. Access the Server Manager Management Console:

   ```
   http://server_name:port/manage
   ```
2. Select the HTML Server instance for which you want to clear the cache from the Instance drop-down list box.
3. Select **JDBj database caches** from the Runtime Metrics section in the left pane.
4. Select the check boxes for the caches to be cleared.
5. Click **Clear Cache**.

   The following caches are available to be cleared:

   - Data Dictionary Glossary Text
   - Data Dictionary Alpha Cache
   - Row Column Cache
   - JDBJ Security Cache
   - JDBJ Service Cache
   - Serialized Objects
   - Menu Cache

25 Setting Up Authorization Security with Security Workbench

Understanding Security Workbench

Use Security Workbench to apply security to JD Edwards EnterpriseOne applications, application versions, forms, and other objects within EnterpriseOne that are described in this chapter. You can apply security for these objects to users, roles, or *PUBLIC.

> **Note:** The Security Workbench is available on both the JD Edwards EnterpriseOne web client and EnterpriseOne Windows client.

When applying object level security, you need to consider how EnterpriseOne checks for security. When a user signs in, the system first checks the user ID for security. If no object security is assigned to the user ID, then it checks the role (if the user is part of a specific role), and then finally it checks *PUBLIC.

You can also use the Security Workbench to apply security to user defined objects (UDOs), which is described in *Managing Security for User Defined Objects*.

In addition to the tools for setting up object security described in this chapter, the Security Workbench provides reports that you can run to perform an audit of Security Workbench security records. See *Running Security Workbench Records Reports* in this guide for more information.

Role-Based Authorization

Administrators prefer to set up security that can be easily managed and maintained. The easiest way to manage object level security in EnterpriseOne is by applying security to roles. Role-based authorization prevents you from having to set up a large number of security records for each individual user. Instead of having to revise multiple security records when a user moves to another position or responsibility, you only have to assign that user to a different role that already contains the required security for that position.

Enforce Security Settings Immediately

JD Edwards EnterpriseOne stores security information in the F00950 table and caches the security information in the web server's memory for the EnterpriseOne web clients and each workstation's memory on EnterpriseOne Windows clients. For Windows client users, changes made to security are applied after the user exits EnterpriseOne and signs back in. For the security changes to take affect on web clients, you must restart the web server or clear the web server's cache using Server Manager. See *"Clear Cache" in the JD Edwards EnterpriseOne Tools Server Manager Guide* for more information.

Managing Exclusive/Inclusive Row Security

This section contains the following topics:

- *Understanding Exclusive/Inclusive Row Security*
- *Exclusive Row Security*
- *Inclusive Row Security*

Understanding Exclusive/Inclusive Row Security

You use row security to either restrict or allow users from viewing, updating, deleting, or adding certain records (rows) to a table. Prior to setting up any kind of row security (whether at the user level, role level, or *PUBLIC level), security administration determines whether your system will use inclusive or exclusive row security. Exclusive row security blocks users from accessing the database for a secured range of values that you define. Inclusive row security allows users to access the database for a valid range of values that you define. You use the User Security application (P98OWSEC) to set up user security.

You use the Row Security application in the Security Workbench application (P00950) to define database values to be excluded or included depending on your JD Edwards EnterpriseOne security configuration. You can set up row security for a user, role, and *PUBLIC. Exclusive row security and inclusive row security are mutually exclusive; you cannot use a combination of the two.

To illustrate exclusive and inclusive row security, assume that user MG5700778 should be able to view records in the Address Book table (F0101) that have a business unit value from 1 through 20 and from 51 through 70. In addition, this user should be able to update records in the Address Book table that have a business unit value from 1 through 20. This user cannot insert or delete any records in the Address Book table. The following examples show the records you must define and the SQL statements that the system performs for both exclusive and inclusive row security.

Exclusive Row Security

This table shows the records that you define using the Row application in Security Workbench when you use exclusive row security to secure your system:

User	Table	Data item	From Value	Thru Value	Add	Change	Delete	View	Alias
MG5700778	*ALL	CostCenter	1	20	N	Y	N	Y	MCU
MG5700778	*ALL	CostCenter	21	50	N	N	N	N	MCU
MG5700778	*ALL	CostCenter	51	70	N	N	N	Y	MCU
MG5700778	*ALL	CostCenter	71	ZZZZZZZZ	N	N	N	N	MCU

This example shows the Select operation that the system performs against the F0101 table:

```
SELECT * FROM TESTDTA.F0101 WHERE ( ABMCU NOT BETWEEN ' 21' AND ' 50'
AND ABMCU NOT BETWEEN ' 71' AND ' ZZZZZZZZ' ) ORDER BY ABAN8 ASC
```

This example shows the Update operation that the system performs against the F0101 table:

```
UPDATE TESTDTA.F0101 SET
ABALKY='MG5700778',ABTAX='456456456',ABALPH='John
Doe',ABDC='JOHNDOE',ABMCU=' 1',ABSIC=' ',ABLNGP=' ',ABAT1='E',ABCM='
',ABTAXC='  WHERE ( ABAN8 = 9999999.000000 ) AND ( ABMCU NOT BETWEEN '
21' AND ' 50' AND ABMCU NOT BETWEEN ' 51' AND ' 70' AND ABMCU NOT
BETWEEN ' 71' AND ' ZZZZZZZZ' )
```

Note: Row security is applied for the range of values that have N in the appropriate Add/Change/Delete/View action.

Inclusive Row Security

This table shows the records that you define using the Row application in Security Workbench when you use inclusive row security to secure your system:

User	Table	Data Item	From Value	Thru Value	Add	Change	Delete	View	Alias
MG5700778	F0101	CostCenter	1	20	N	Y	N	Y	MCU
MG5700778	F0101	CostCenter	51	70	N	N	N	Y	MCU

This example shows the Select operation that the system performs against the F0101 table:

```
SELECT * FROM TESTDTA.F0101 WHERE ( ( ABMCU BETWEEN ' 1' AND ' 20' OR
ABMCU BETWEEN ' 51' AND ' 70' ) ) ORDER BY ABAN8 ASC
```

This example shows the Update operation that the system performs against the F01010 table:

```
UPDATE TESTDTA.F0101 SET ABALKY=' ',ABTAX='546',ABALPH='John
Doe',ABDC='JOHNDOE',ABMCU=' 60',ABSIC='
',ABUSER='MG5700778',ABPID='EP01012',ABUPMJ=101214,ABJOBN='DEN123456',
ABUPMT=154030.000000 WHERE ( ABAN8 = 6864221.000000 ) AND ( ABMCU
BETWEEN ' 1' AND ' 20' )
```

Note: The presence of a single record or a set of security records in the Security Workbench table (F00950) with all N values for one or more operations for a table and data dictionary combination will disallow that user from performing that particular operation on the table.

Note: Row Security is applied for range of values that have Y in the Add/Change/Delete/View action

As illustrated in the examples, when you define data access security using exclusive row security, you identify a range of values that are to be secured from the user. When you define data access security using inclusive row security, you identify a range of values that the user can access. Depending on your security setup, inclusive row security can increase performance over exclusive row security. The reason for the performance increase is due to the select and update statements that the middleware generates. Performance can be improved if the use of inclusive row security results in a small range of valid values in the row security application rather than specifying a large range of secured values in the row security application to use exclusive row security.

Activating Inclusive Row Security

The system assumes Exclusive Row Security unless you specify inclusive row security.

Use these steps to activate inclusive row security:

1. Enter `P00950` in the Fast Path to access the Security Workbench.
2. On the Work With User/Role Security form, select **Exclusive/Inclusive** from the Form menu.
3. On the Inclusive/Exclusive Row Security form, select the **Inclusive Row Security** option.
4. Click **OK**.

If your system is prior to JD Edwards EnterpriseOne Tools Release 8.9, you must manually enter a record in the Security Workbench table using SQL to indicate to your system that inclusive row security is to be used. Use this Insert SQL statement as an example:

```
Insert into SYS7333.F00950 (FSSETY, FSUSER, FSOBNM, FSDTAI, FSFRDV,
FSSY, FSATN3) Values(' ','EXCLUSIVE',' ', ' ', ' ', ' ' , '1')
```

Creating Security Overrides

This section contains the following topics:

- *Understanding Security Overrides*
- *Adding Security Overrides*

Understanding Security Overrides

Security overrides operate as exceptions to existing security records. They specify that users are *unsecured* from an EnterpriseOne object. In other words, security overrides allow users access to a particular object, even if another security record in the system specifies that access is not allowed.

Security overrides enable you to create object security more efficiently, with fewer security records to manage. For example, you might have a scenario that requires securing four out of five versions of an application from a group of users. Instead of creating four security records to prevent users from accessing each of the four versions, you can create two security records to achieve the same result. First, you would create a security override for the application version that you want users to access. This security override would specify that this version is not secured. These are the high level steps to create security overrides in Security Workbench:

1. Create a security record for the version, making sure that the security options are cleared.
2. Create a security record that secures users from accessing the application, including all versions of the application. In Security Workbench, you would select the application and then select the Run security option, which secures users from running the application.

As a result, when users try to access the application version, the security override for the version operates as an exception to the second application security record, allowing users access to the version of the application. All other versions of the application are secured.

You can create security overrides for these JD Edwards EnterpriseOne objects:

- Applications
- Actions
- Processing options
- Tabs
- Hyper exits
- External calls
- Push buttons, links, and images
- Media objects

Creating security overrides simplifies the process of applying security to various EnterpriseOne items. The following table provides some scenarios in which you could use security overrides to set up your security:

Scenario	Method
Allow a user or group of users access to a single form in an application. These users are otherwise restricted from using the application.	To set up: 1. Create a security override for the form. 2. Create a security record to prevent users from accessing the application.
Secure users from using all but one push button on a form in an application. This security shall apply to all versions of the application as well.	To set up: 1. Create a security override for the push button. 2. Create a security record to prevent users from using all push buttons on the form.
Allow only one user in a role access to an external application.	To set up: 1. Create a security override for the user that gives the user access to the external application. 2. Create a security record that prevents the role from accessing the external application.
Secure users from all action buttons except Add and Copy on a form in a particular version of an application.	To set up: 1. Create a security override to specify that Add and Copy action buttons are not secured on a form in a particular version of an application. 2. Create a security record to secure all actions on the form.

Before you can create a security override for an EnterpriseOne object, you must first understand how a standard security record for the object is created in Security Workbench. See the appropriate sections in this chapter for instructions on how to apply security to EnterpriseOne objects such as applications, processing options, tabs, and media objects.

Adding Security Overrides

Enter **P00950** in the Fast Path.

1. On Work With User/Role Security, select the **Form** menu, **Set Up Security**, and then select the menu for the type of object for which you want to create a security override.
2. On the security form, enter the user or role ID in the User / Role field.
   Enter a complete user or role, which includes *PUBLIC.
3. In the Display UnSecured Items region, complete the appropriate fields, and then click **Find**.
   This step provides a list of unsecured items for the user, role, or *PUBLIC in the UnSecured node.
4. Expand the UnSecured node to view the individual applications or versions, and the forms associated with each, that do not already have security set for them.
   After you expand the node, each item that you select appears in the grid.
5. Select the item in the node that you want to create a security override for.
6. In the Create with region, make sure that the security options are cleared or not selected.
7. Drag the item from the UnSecured node to the Secured node.
   This action creates a security override for the user or role that can operate as an exception to a another security record for the user or role.

Managing Application Security

This section contains the following topics:

Understanding Application Security

Application security enables you to secure these types of items from users:

- Applications
  When you secure an application, you secure all versions and forms associated with the application.
- Versions
  You can secure access to a version of an application while leaving other versions available to the user.
- Forms
  You can secure access to a single form in an application or application version.

You can secure users from running or installing (or both) a particular application, version, or form within an application. You cannot define application security at the subform level. As an alternative, you could define column security at the form level (power form level) and every instance of the data dictionary item (either on the power form header or subform grid) follows the defined security.

This section also explains how to add a *ALL object and change all of the applications for a particular user or role from unsecured to secured.

For additional information, refer to the white paper "JD Edwards EnterpriseOne HCM Applications Data Security" on the Oracle Learning Library site.

https://apexapps.oracle.com/pls/apex/f?p=44785:24:0::::P24_CONTENT_ID,P24_PREV_PAGE:27041,1

Understanding Application Security for Mobile Applications

You can configure application security for EnterpriseOne mobile enterprise applications.JD Edwards EnterpriseOne uses a "secure by default" security model which means that users cannot access a mobile application unless a security record exists that authorizes access.

In Security Workbench, the only application security option that applies to mobile applications is the "Run" security option.

Before you set up security for mobile applications, you must define which version of the mobile application mobile users will use. Then you apply application security to the mobile application version.

See *"Setting Up the System to Use Mobile Applications" section in the JD Edwards EnterpriseOne Applications Mobile Enterprise Applications Implemenation Guide* for a complete list of implementation tasks required to set up mobile enterprise applications.

Reviewing the Current Application Security Settings for a User or Role

Enter **P00950** in the Fast Path.

1. On Work With User/Role Security, select the **Form** menu, **Set Up Security**, **Application**.
2. On the Application Security form, enter the user or role ID in the User / Role field.

   Enter a complete user or role, which includes *PUBLIC but not wildcards.

3. In the Display UnSecured Items region, complete the appropriate fields to determine which items have already been secured for the user or role, and then click **Find**:
   - Application

     Enter an application name, such as `P01012`. You can also enter `*ALL` to display all applications.
   - Version

     Enter a version name, such as `ZJDEC0001`, if you want to check only a specific version of an application. You can also use an asterisk to display all versions.
   - Form Name

     Enter a form name, such as `W01012A`. You can also enter an asterisk to display all forms.
4. Expand the Secured node to view the security settings for the user or role in the detail area.

Adding Security to an Application

Enter **P00950** in the Fast Path.

> **Note:** You cannot secure the Data Browser application using the Application Security form. Security Workbench provides a separate option for securing this application. See *Managing Data Browser Security*.

1. On Work With User/Role Security, select the **Form** menu, **Set Up Security**, **Application**.
2. On the Application Security form, enter the user or role ID in the User / Role field.

   Enter a complete user or role, which includes ***PUBLIC** but not wildcards.
3. In the Display UnSecured Items region, complete the appropriate fields, and then click **Find**.
   - Application
   - Version

     Enter a particular version of the application that you entered in the Application field. If you leave this field blank, the system displays all versions associated with the application in the UnSecured node.
   - Product Code

     Enter a product code to display all applications, versions, and forms associated with a particular product code. This field does not work in conjunction with the Application or Version fields.

     The search results appear under the UnSecured node.
4. Expand the UnSecured node to view the individual applications or versions, and the forms associated with each, that do not already have security set for them.

   After you expand the node, the individual items also appear in the grid.

5. In the Create with region, select one or both of these security options:
   - Run Security

     Select this option to secure users from running the application.
   - Install Security

     Select this option to prevent the just-in-time installation (JITI) of anything necessary to run the application.
6. Complete one of these steps:
   - Drag applications, versions, or forms from the UnSecured node to the Secured node.
   - From the Row menu, select **All Objects** to move all applications to the Secured node.
   - From the Row menu, select **Secure to All** to move all objects that are under the UnSecured node to the Secured node.

     If you secured an individual form, only the form appears under the Secured node. If you secured an application or version, the application or version and the forms associated with each appear under the Secured node.
7. To change the security on an item, select the item under the Secured node, select the appropriate security option, and then, from the Row menu, select **Revise Security**.

   In the grid, the values under the Run and Install fields change accordingly.

Securing a User or Role from All JD Edwards EnterpriseOne Objects

Enter `P00950` in the Fast Path.

1. On Work With User/Role Security, select the **Form** menu, **Set Up Security**, **Application**.
2. On the Application Security form, enter the user or role ID in the User / Role field.

   Enter a complete user or role, which includes *PUBLIC but not wildcards.
3. In the Display UnSecured Items area, enter `*ALL` in the Application field to select `all` JD Edwards EnterpriseOne objects, and then click **Find**.
4. Expand the UnSecured node and then click ***ALL** in the detail area.
5. In the Create with region, select one or both of these options:
   - Run Security

     Use this option to secure users from running all applications.
   - Install Security

     Use this option for JITI only.
6. Complete one of these steps:
   - Drag ***ALL** from the UnSecured node to the Secured node.
   - From the Row menu, select **All Objects** to move *ALL to the Secured node.
   - From the Row menu, select **Secure to All** to move *ALL from UnSecured node to the Secured node.

Removing Security from an Application

Access the Application Security form.

On the Application Security form, perform one of these steps:

- Under the Secured node, select an application, version, or form and click **Delete**.
- Drag an application, version, or form from the Secured node to the UnSecured node.
- Select **Remove All** from the Row menu to move *all* items from the Secured node to the UnSecured node.

Managing Action Security

This section contains the following topics:

- *Understanding Action Security*
- *Reviewing the Current Action Security Settings*
- *Adding Action Security*
- *Removing Action Security*

Understanding Action Security

Action security enables you to secure the buttons that enable users to perform particular actions, such as adding, deleting, inquiring, revising, or copying a record. These buttons typically reside on the toolbar in a form. Do not confuse these buttons with buttons that are located on other parts of a form.

You can define action security at the application, version, and form level. You cannot define action security at the subform level. As an alternative, you could define column security at the form level (power form level) and every instance of the data dictionary item (either on the power form header or subform grid) follows the defined security.

Oracle recommends that after you add action security to an application, you should test the application to make sure that the security works as desired. For example, adding action security to an Add or OK button in some applications that have editable grids does not prevent users from adding new records or modifying existing ones. For these applications, you would have to add additional security to the application as well.

Note:

- *Managing Push Button, Link, and Image Security*.
- *Managing Hyper Exit Security*.

Reviewing the Current Action Security Settings

Enter `P00950` in the Fast Path.

1. On Work With User/Role Security, select the **Form** menu, **Set Up Security**, **Action**.

2. On the Action Security form, enter the user or role ID in the User / Role field and click Find.

   You can enter `*PUBLIC` but not wildcards.

   Current action security settings for the user or role appear under the Secured node in the tree.
3. To see if an action security is applied to a particular application, version, or form, complete a combination of these fields in the Display Secured Item region, and then click **Find**:
   - Application

     Enter an application name, such as `P01012`.
   - Version

     Enter a version of the application entered in the Application field to see if action security is applied to the version.
   - Form Name

     Enter a form name, such as `W01012A`.
4. Expand the Secured node and click a secured item to view the current security settings for the user or role in the detail area.

Adding Action Security

Enter `P00950` in the Fast Path.

1. On Work With User/Role Security, select the **Form** menu, **Set Up Security**, **Action**.
2. On the Action Security form, enter the user or role ID in the User / Role field and click **Find**.

   You can enter `*PUBLIC` but not wildcards.

   Current action security settings for the user or role appear under the Secured node in the tree.
3. To find the applications, versions, or forms to which you want to apply action security, complete any of these fields under the Display UnSecured Items heading, and then click **Find**:
   - Application

     Enter an application name, such as `P01012`. Enter `*ALL` to display all applications.
   - Version

     Enter a version of the application you entered in the Application field. If you leave this field blank, all versions associated with the application will appear in the UnSecured node.
   - Product Code
4. Expand the Unsecured node to view individual applications, versions, and forms in the detail area.
5. In the Create with region, select any of these options:
   - Change
   - Add
   - Delete
   - OK/Select
   - Copy

- Scroll To End

  When you select the OK/Select function, both the Select and OK buttons will be disabled on forms regardless of the setting for any of the other functions. The reason that separate options exist for OK/Select and the other functions is to allow a user to select records from a Find/Browse or Inquiry form but not be able to perform those actions that you secured. For example, a valid setup would be to set OK/Select to **Y** and set Change to **N**. The user will be able to select records but not change them. However, if you set OK/Select to **N** and Change to **Y**, the OK and Select buttons will be disabled even if the form is in update mode.

6. To secure the actions on an application, version, or form, perform one of these steps:
   - Drag the application, version, or form from the UnSecured node to the Secured node.
   - From the Row menu, select **All Objects** to move all items to the Secured node.
   - From the Row menu, select **Secure to All** to move all objects under the UnSecured node to the Secured node.

     For example, to set delete security on an application, select the Delete option. Next, drag the application from the UnSecured node to the Secured node. The detail area will reflect the delete security that you set for this application, which means that the user you entered cannot perform the delete action on this application.

     The applications or forms now appear under the Secured node and they have the appropriate action security.
7. To change the security on an item, select the item under the Secured node, select the appropriate security option, and then, from the Row menu, select **Revise Security**.

   In the grid, the values for the security options change accordingly.

Removing Action Security

Enter `P00950` in the Fast Path.

1. On Work With User/Role Security, select the **Form** menu, **Set Up Security**, **Action**.
2. On the Action Security form, enter the user or role for which you want to change action security in the User / Role field, and then click **Find**.
3. To delete action security from an application, version, or form, do one of these:
   - Under the Secured node, select an application, version, or form and click Delete.
   - Under the Secured node, drag an application, version, or form from the Secured node to the UnSecured node.
   - Select **Remove All** from the Row menu to move *all* applications and forms from the Secured node to the UnSecured node.

Managing Row Security

This section contains the following topics:

- *Understanding Row Security*

Understanding Row Security

Row security enables you to secure users from accessing a particular range or list of data in any table. Use row security sparingly because it can adversely affect system performance. Additional processing occurs for each data item that you set with row security.

You can set up row security at three levels:

- User
- Role
- *PUBLIC

EnterpriseOne looks for row security first at the user level, then at the role level, and then at the *PUBLIC level. If you set any of the security at a higher level, such as at the user level, the software ignores lower-level security settings, such as the group or *PUBLIC levels.

Before you set up row security for an item in a table, you should verify that the item is actually in that table. For example, the F0101 table contains the data item AN8. Therefore, you can set up row security for that item. However, the same table does not contain data item PORTNUM. Setting row security on this item for the F0101 table has no effect.

You set up row security on a table, not on a business view. You should verify that the object that you want to secure uses a business view over a table containing the object. For example, the Work With Environments application (P0094) uses business view V00941 over the F00941 table. You could secure the data item RLS (Release) because it is in the F00941 table. On the other hand, the same item is not in the F0094 table. If you attempt to secure the item on the F0094 table, data item RLS is not secured.

> **Note:** You can find the tables, applications, forms, business views, and so on that use a data item by launching the Cross Reference application (P980011) after you build cross-reference tables (F980011and F980021).

Prerequisite

Before you can set up row security, you must activate row security in Data Dictionary Design.

See *"Creating a Data Dictionary Item" in the JD Edwards EnterpriseOne Tools Data Dictionary Guide* .

Setting Up Data Dictionary Spec Files

After you activate row security in Data Dictionary Design, sign out of EnterpriseOne and delete the following spec files, which as of Tools Release 9.2.6.0 are in the \pathcode\spec\package directory of the Enterprise Server:

- dddict.xdb
- dddict.ddb

- ddtext.xdb
- ddtext.ddb
- glbltbl.xdb
- glbbltbl.ddb

If you do not use data dictionary replication (prior to release 9.2.2 only), you must delete these spec files for each path code directory on your machine and every workstation, including the enterprise server, where this security needs to be activated. These spec files are automatically rebuilt as data dictionary items are referenced the next time the user signs in to EnterpriseOne when just-in-time installation (JITI) is enabled for the environment.

Note: If your system is prior to JD Edwards EnterpriseOne Applications Release 8.11, and you are using terminal servers in an environment that does not use JITI, you must rebuild the data dictionary and global table spec files using R92TAM and R98CRTGL to get the changed data dictionary information to the terminal servers

Adding Row Security

Enter `P92001` in the Fast Path.

1. On Work With Data Items, click **Find**.

   Note: You can enter search criteria in the Search Description field and the query by example (QBE) row to narrow your search.

2. Select the data item that you want to secure, and click **Select**.

   The Data Item Specifications form appears.
3. On the Item Specifications tab, select the **Row Security** option and click **OK**.

   This option must be selected for row security to work.
4. Click **OK**.
5. Exit the data dictionary application.
6. In Solution Explorer, enter `P00950` in the Fast Path and press Enter.
7. On the Work With User/Role Security form, select the **Form** menu, **Set Up Security**, **Row**.
8. On the Row Security form, complete the User / Role field and then click **Find** to display current row security.
9. Complete these fields, either in the first open detail area row (to add security) or in a pre-existing detail area row (to change security):
   - Table

     You can enter `*ALL` in this field.
   - Data Item

     This field is required.
   - From Value

     This field is required.
   - Thru Value
   - Add
   - Change

- Delete
- View

10. Click **OK** to save the security information.

Removing Row Security

Enter `P00950` in Fast Path.

1. On the Work With User/Role Security form, select an object.
2. From the Form menu, select **Set Up Security**, **Row**.
3. On the Row Security form, complete the User / Role field and click **Find**.

   > **Note:** If you accessed the Row Security form from the Work With User/Role Security form for a specific record, the user or role associated with the security record appears in the User / Role field by default.

4. Select the security record or records in the detail area, and then click **Delete**.
5. On Confirm Delete, click **OK**.
6. Click **OK** when you finish deleting row security.

   If you do not click OK after you delete the row security records, the system does not save the deletion.

Managing Column Security

This section contains the following topics:

- *Understanding Column Security*
- *Adding Column Security*
- *Removing Column Security*

Understanding Column Security

This section explains how to add and revise column security. You can secure users from viewing a particular field or changing the value for a particular field. This item can be a database field, or a field that is defined in the data dictionary but is not in the database.

> **Note:** You can find the tables, applications, forms, business views, and so on, that use a data item by launching the Cross Reference application (P980011) after you build the cross-reference tables (F980011and F980021).

You can set up column security on a table, an application, an application version, or a form. Even if an application uses a business view that does not contain the data item that you want to secure, you can still secure it, as long as the item appears on a form in the application.

Column Security Options

When you use Column Security you can set View, Add, and Change options to secure a field. For the field to appear on a table, application, application version, or form, the View option must be set to **Y**. When the View option is set to **N** for a

field, that field does not appear on the object. Add and Change options depend on the View option being set to **Y** for the field. The Add and Change options are independent of each other.

You can set the View and Add options to **Y** and the Change option to **N**. With security defined in this manner, the field appears on the object and is enabled when the user enters the object in add mode. If the user enters the object in update mode, the field appears but is disabled.

You can set the View and Change options to **Y** and the Add option to **N**. With security defined in this manner, the field appears on the object and is enabled when the user enters the object in update mode. If the user enters the object in add mode, the field appears but is disabled.

You can set all three options to **Y**. With security defined in this manner, the field appears on the object and is enabled in both add and update mode.

Column Security on a Table

Before you set up column security on a table, do these:

- Verify that the object that you want to secure is in the table.
- Verify that the object that you want to secure is part of an application that uses a business view over a table containing the object.
- Verify that the object that you want to secure uses a business view that includes the column containing the object.

For example, if you want to apply column security to data item RLS (Release Number) in the F00941 table, RLS must be an item in that table, and it must also be part of an application using a business view over that table. Finally, the business view over the F00941 table must include a column containing the data item RLS.

If all of these conditions are met, you can successfully apply column security to the data item. Setting column security on a table also means that you set security on the data item for any other applications that use the F00941 table.

Column Security on an Application

Before you set up column security on an application, do these:

- Verify that the object that you want to secure is in the application.
- Verify that you are securing the correct data item in an application (data item descriptions can be similar, if not identical).

For example, if you want to apply column security to data item UGRP (UserRole) in the Object Configuration Manager application (P986110), you first verify that the item is in the application. Because it is in the application, you can apply security to the data item. However, note that data items UGRP, MUSE, USER, and USR0 all contain the identical data description of *User ID*. Verify the item by its alias, not by its data description.

Column Security on an Application Version

You can secure users from using columns (or fields) in a version of an application. When you secure a column in a version, the system secures the column in all forms associated with that application version.

Before you set up column security on an application version, do these:

- Verify that the object that you want to secure is in the version of the application.
- Verify that you secure the correct data item in an application (data item descriptions can be very similar, if not identical). Verify the item by its alias, not by its data description.

Column Security on a Form

Security Workbench enables you to secure the column in one particular form, either in an application or in a version of an application.

Before you set up column security on a form, do these:

- Verify that the object that you want to secure is in the form.
- Verify that you secure the correct data item in the form (data item descriptions can be very similar for different data items).

Adding Column Security

Enter `P00950` in Fast Path.

1. On the Work With User/Role Security form, select the **Form** menu, **Set Up Security**, **Column**.
2. On the Column Security form, complete the User / Role field, and then click **Find** to display current column security for the user or role.
3. To add new security, go to the last row of the detail area and enter information into any of these fields:
   - Table
   - Application
   - Version

     If you want to add column security to a particular version, enter a version of the application that you entered in the Application field.
   - Form Name

     You can enter `*ALL` in any of these fields; however, after *ALL is entered for a table, application, or form for a specific data item, you cannot enter *ALL again for that data item.
4. Complete these fields:
   - Data Item
   - View

     If the value for View is N, the data item will not appear on any of the objects identified in Step 3, making Add and Change functions obsolete.
   - Add
   - Change
5. To change security, change the row values in the detail area.
6. Click **OK** to save the security information.

Removing Column Security

Enter `P00950` in the Fast Path.

1. On the Work With User/Role Security form, select the **Form** menu, **Set Up Security**, **Column**.
2. On the Column Security form, complete the User / Role field, and then click **Find**.

> **Note:** If you accessed the Column Security form from the Work With User/Role Security for a specific record, the user or role associated with the security record appears in the User/Role field by default.

3. Highlight the security record or records in the detail area and click **Delete**, and then click **OK** on Confirm Delete.
4. Click **OK** when you finish deleting column security.

   If you do not click OK after you delete the security records, the system does not save the deletion.

Managing Processing Option and Data Selection Security

This section contains the following topics:

- *Understanding Processing Option Security*
- *Understanding Data Selection Security*
- *Reviewing the Current Processing Option and Data Selection Security Settings*
- *Adding Security to Processing Options and Data Selection*
- *Removing Security from Processing Options and Data Selection*
- *Using R009505 to Update Data Selection Security*

Understanding Processing Option Security

You can secure users from changing, prompting for values, and prompting for versions of specific processing options. By itself, setting security that prohibits users from prompting for versions does not prevent them from changing values in the processing option. If you do not want users to use processing option values, you might want to set security so that users are secured from the "prompt for" value and "prompt for" versions.

For example, to set prompt-for-values security, which also automatically sets change security, select the Prompt for Values option. Next, drag one application at a time from the UnSecured node to the Secured node. The detail area reflects the prompt-for-values and change security that you set for these applications. This procedure means that the user you entered cannot modify processing options on any applications that you placed in the Secured node.

This task also explains how to add a *ALL object and how to move all of the applications for a particular user or role from unsecured to secured.

Understanding Data Selection Security

You can secure users from modifying, adding, deleting, and viewing the data selection for batch applications or specific versions of batch applications. This security applies to the data selection during submission of a batch application (or report).

Implementation Considerations

Data selection security only applies to web clients. You can set up data selection security by running the Security Workbench application on the Windows client. However, the security is only enforced for end users submitting

batch applications from the web client. It is not enforced for other means of launching reports, such as RUNUBE and RUNUBEXML commands or the scheduler.

The Data Selection row exit on the Work with Batch Versions form allows a user to modify the data selection for a version or report. Oracle recommends that the EnterpriseOne security administrator secures the Data Selection row exit using existing hyper exit security in addition to setting up proper data selection security.

For example, data selection security is set up for a user on a batch application version so that the user cannot modify existing rows but can add new rows. However, the user can access the Data Selection row exit and use this row exit to add rows to the existing data selection. When the user clicks OK, the data selection specification is saved to the version. When the user takes the Data Selection row exit again, all rows become existing rows that are secured out. As a result, he cannot modify rows that he just added.

You should also consider using action security to secure the ability to add and copy versions of a batch application. Or you can set data selection security at the batch application level rather than version level. In this case, a new user-created version that was created through add or copy will still have the same data selection security.

Data Selection Security Options

The available security settings related to data selections are:

Security Setting	Description
Prompt for Data Selection	This setting prevents a user from viewing the data selection screen when submitting a report or version. The data selection criteria defined in the version are used for submission.
Full Access for Data Selection	This setting prevents a user from having a full set of the editing capabilities on the data selection screen. Specifically, it prevents a user from deleting any existing data selection criteria. When this setting is checked, two additional settings "Modify for Data Selection" and "Add for Data Selection" are enabled. All three settings can be used in combination.
Modify for Data Selection	This setting prevents a user from editing or deleting existing data selection criteria defined for a report or version. It also prevents a user from adding new data selection criteria with an OR operator, in effect either expanding or changing existing criteria. This setting is made available only when the user is not granted with Full Access for Data Selection.
Add for Data Selection	This setting prevents a user from adding new data selection criteria. This setting is made available only when the user is not granted with Full Access for Data Selection. This setting can be used in combination with the Modify for Data Selection setting.

All of the security settings can be set at the specific user, role, or *PUBLIC level for any report version or report.

Security Hierarchy

When multiple security records exist, the system applies security by following the existing security hierarchy:

1. Version level security for user.
2. Batch application level security for user.
3. *ALL level security for user.
4. Version level security for group.
5. Batch application level security for group.
6. *ALL level security for group.
7. Version level security for *PUBLIC.

8. Batch application level security for *PUBLIC.
9. *ALL level security for *PUBLIC.

Once a security record is found, the system stops searching for lower priority records.

Note: The JAS Server (EnterpriseOne HTML Server) resolves the security entries for the group based on the role sequence number, and only returns one record for all groups at runtime.

Data Selection Security Scenarios

This table lists the possible data selection security scenarios. "X" indicates that the specified check box is checked in the Security Workbench application:

Scenario	Prompt for Data Selection	Full Access Data Selection	Modify Data Selection	Add Data Selection
Full access to data selection.	N/A	N/A	N/A	N/A
No access to data selection form. User receives error when he tries to access data selection.	X	Grayed out and checked by default	Grayed out and checked by default	Grayed out and checked by default
Read-only access.	N/A	X	X	X
User can only add new data selection rows with AND operator. User cannot modify or delete existing data selection rows.	N/A	X	X	N/A
User can only modify the right operand value for existing data selection rows. User cannot add new data selection rows or delete existing rows.	NA	X	N/A	X
User can modify existing rows and add new rows with the 'AND' operator. User cannot delete existing rows.	N/A	X	N/A	N/A

Reviewing the Current Processing Option and Data Selection Security Settings

Enter `P00950` in the Fast Path.

1. On the Work With User/Role Security form, select **Set Up Security**, **Proc Opt Data Sel**.
2. On the Processing Option and Data Selection Security form, enter a user or role ID in the User / Role field. Enter a complete user or role, which includes `*PUBLIC` but not wildcards.
3. In the Display Secured Item region, complete these fields and then click **Find**:

- Application

  Enter a batch application name, such as `R0006P`. Enter `*ALL` to display all applications.
- Version

  Enter a version of the application that you entered in the Application field.

  Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications. After you expand the node, the applications that are secured also appear in the detail area.

Adding Security to Processing Options and Data Selection

Enter `P00950` in the Fast Path.

1. On the Work With User/Role Security form, select the **Form** menu, **Set Up Security**, **Proc Opt Data Sel**.
2. On the Processing Option and Data Selection Security form, enter the user or role ID in the User / Role field and then click **Find**.

   Enter a complete user or role, which includes *PUBLIC but not wildcards.
3. In the Display UnSecured Items region, complete the appropriate fields and then click **Find**:

   - Application

     Enter an application name, such as `R0006P`. Enter `*ALL` to display all applications.
   - Version

     You can enter a particular version of the application that you entered in the Application field. If you leave this field blank, all versions associated with the application will appear in the UnSecured node.
   - Product Code
   - UBEs Only

     Select this check box to view only batch applications.

     You must perform this step before you can add new security. This step provides a list of applications from which you can apply processing option or data selection security.

     The search results appear under the UnSecured node. Expand the node to view applications (interactive and batch) and menus with interactive or batch applications. After you expand the node, the applications appear in the detail area.

     For example, to set security on applications within the 00 product code, you enter **00** in the Product Code field and click Find. All of the applications (interactive and batch) attached to product code 00 appear after you expand the UnSecured node.

4. In the Create with region, select one or more of these options and drag applications from the UnSecured node to the Secured node:
   - Change
   - Prompt for Values

     When you select this option, you automatically activate the Change option.
   - Prompt for Versions
   - Prompt for Data Selection
   - Full Access Data Selection

     When you select this option, you automatically activate the following two options:
   - Modify Data Selection
   - Add Data Selection

     See Data Selection Security Scenarios.
5. Perform one of these actions:
   - Drag applications from the UnSecured node to the Secured node.
   - From the Row menu, select **All Objects** to move all applications to the Secured node.
   - From the Row menu, select **Secure to All** to move all objects under the UnSecured node to the Secured node.

     The applications now appear under the Secured node and have the appropriate security.
6. To change the security on an item, select the item under the Secured node, select the appropriate security option, and then, from the Row menu, select **Revise Security**.

   In the grid, the values for the security options change accordingly.

Removing Security from Processing Options and Data Selection

Enter `P00950` in the Fast Path.

1. On the Work With User/Role Security form, select the **Form** menu, **Set Up Security**, **Proc Opt Data Sel**.
2. On the Processing Option and Data Selection Security form, enter a user or role ID for which you want to remove processing option or data selection security in the User / Role field.

   Enter a complete user or role, which includes `*PUBLIC` but not wildcards.
3. Click **Find**.

   Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications. After you expand the node, the applications that are secured also appear in the detail area.
4. Perform one of these steps:
   - Under the Secured node, select an application or application version and click **Delete**.
   - Under the Secured node, drag an application or application version from the Secured node to the UnSecured node.
   - On the Row menu, select **Remove All** to move *all* items from the Secured node to the UnSecured node.

Note: *Click here to view a recording of this feature.*

Using R009505 to Update Data Selection Security

The data selection security records are stored in the security table as security type 5. You can use the R009505 batch application to clean up any existing security type 5 records.

The R009505 runs over the F00950 table with data selection on records of Security Type 5 (Processing Option and Data Selection Security). These records must have a value in the Object Name field that is a batch application or *ALL (since Security Type 5 can be set up for interactive application objects as well, those will be ignored by this batch application.) The batch application can be run in Proof or Final Mode where Final Mode will update the F00950 table records according to the values in the processing options. The F00950 table will be updated as follows given the processing option values:

PO	Y or N	Actual Record
Prompt for Data Selection	Y	Y
Full Access Data Selection	Y	Y
Modify Data Selection	Y	Y
Add Data Selection	Y	Y
Prompt for Data Selection	N	N
Full Access Data Selection	Y	N
Modify Data Selection	Y	N
Add Data Selection	Y	N
Prompt for Data Selection	N	N
Full Access Data Selection	N	N
Modify Data Selection	Y	N
Add Data Selection	Y	N
Prompt for Data Selection	N	N
Full Access Data Selection	N	N
Modify Data Selection	N	N
Add Data Selection	Y	N
Prompt for Data Selection	N	N
Full Access Data Selection	N	N
Modify Data Selection	N	N

PO	Y or N	Actual Record
Add Data Selection	N	N
Prompt for Data Selection Full Access Data Selection Modify Data Selection Add Data Selection	Y N N N	Y N N N
Prompt for Data Selection Full Access Data Selection Modify Data Selection Add Data Selection	Y Y N N	Y Y Y Y

Managing Tab Security

This section contains the following topics:

- *Understanding Tab Security*
- *Adding Tab Security*
- *Removing Tab Security*

Understanding Tab Security

You can secure users from changing the name of the tab and viewing the form that you call by using the tab. For example, to set up change security, select the Change option. Next, drag tabs one at a time from the UnSecured node to the Secured node. The detail area reflects the changed security that you set for the tabs. This security means that the user you entered cannot change the tabs that you dragged to the Secured node.

> **Note:** If you secure a user from an application, you cannot also secure the user from certain tabs on a form in that application. This restriction prevents redundant double security. Similarly, if you secure a user from a tab, you cannot secure the user from the application that contains the tab.

You can define Tab security at the application, version, and form level. You cannot define Tab security at the subform level. As an alternative, you could define column security at the form level (power form level) and every instance of the data dictionary item (either on the power form header or subform grid) follows the defined security.

> **Note:** Portlets are handled by the system as if they are subforms; therefore, portlets have the same Tab security limitation.

Adding Tab Security

Enter `P00950` in the Fast Path.

1. On the Work With User/Role Security form, select the **Form** menu, **Set Up Security**, **Tab**.
2. On the Tab Exit Security form, complete these fields and click **Find**:
   - User / Role

     Enter a complete user or role, which includes *PUBLIC but not wildcards.
   - Application

     You can view security for a specific application or enter `*ALL` to display all applications.

     Current security settings for the user or role appear under the Secured node in the tree. Expand the nodes to view the secured tabs. After you expand the node, the secured tabs also appear in the grid.
3. Complete *only one* of these fields in the Display UnSecured Items region and click **Find**:
   - Application

     Enter `*ALL` in this field to select *all* JD Edwards EnterpriseOne objects.

     In the detail area, this special object appears as *ALL and displays the security that you defined for the object, such as Run Security or Install Security. The *ALL object acts as any other object, and you can use the Revise Security and Remove All options from the Row menu.
   - Product Code

     You must perform this step before you can add new security. This step provides a list of applications from which to select.

     The search (application or product code) appears under the UnSecured node. Expand the node to view applications (interactive and batch) and the associated tabs. After you expand the node, the applications or tabs also appear in the detail area.

     For example, to set security for tabs in applications within the 00 product code, you enter `00` in the Product Code field and click **Find**. All of the applications (interactive and batch) attached to product code 00 appear after you expand the UnSecured node.
4. In the Create with region, select one or more of these options:
   - Change

     Select this option to prohibit a user or role from changing information on the tab page.
   - View

     Select this option to hide the tab from the user or the role.
5. Drag tabs from the UnSecured node to the Secured node.

   These tabs now appear under the Secured node.
6. To change the security on an item, select the item under the Secured node, select the appropriate security option, and then, from the Row menu, select **Revise Security**.

   In the grid, the values for the security options change accordingly.

Removing Tab Security

Enter `P00950` in the Fast Path to access the Work With User/Role Security form.

1. From the Form menu, select **Set Up Security**, **Tab**.
2. On the Tab Exit Security form, complete these fields and click **Find**:
   - User / Role

     Enter a complete user or role, which includes *PUBLIC but not wildcards.
   - Application

     You can view security for a specific application or enter `*ALL` to display all applications.

     Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the secured tabs. After you expand the node, the secured tabs also appear in the grid.
3. Perform one of these steps:
   - Under the Secured node, select a tab and then click **Delete**.
   - Under the Secured node, drag a tab from the Secured node to the UnSecured node.
   - On the Row menu, select **Remove All** to move all tabs from the Secured node to the UnSecured node.

Managing Hyper Exit Security

Menu bar exits, also referred to as hyper exits, call applications and allow users to manipulate data. You can secure users from using these exits. Hyper exit security also provides restrictions for menu options. This section contains the following topics:

- *Adding Hyper Exit Security*
- *Removing Hyper Exit Security*

Adding Hyper Exit Security

Enter **P00950** in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Hyper Exit Security.
2. On the Hyper Exit Security form, complete these fields and click **Find**:
   - User / Role

     Enter a complete user or role ID, which includes *PUBLIC but not wildcards.
   - Application

     View security for a specific application. Enter `*ALL` to display all applications.

     Current security settings for the user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as interactive and batch. After you expand the node, the secured hyper-button exits also appear in the detail area.

3. In the Display Unsecured Items region, complete only one of these fields to locate the applications to which you want to apply exit security, and click **Find**:
   - Application

     If you enter *ALL in this field and select the Run Security option, all action buttons (except Close and Cancel on the web client only) including every exit under the Form, Row, and Tools options are disabled. To avoid disabled action buttons, apply Hyper Exit security at the individual application level.
   - Product Code

     You can search for all of the applications within a product code. For example, to set security on hyper-buttons in applications within the 00 product code, you enter `00` in the Product Code field and click **Find**. All of the applications (interactive and batch) attached to product code 00 appear after you expand the UnSecured node.

     The search (application, product code, or menu) appears under the UnSecured node. Expand the node to view applications (interactive and batch) and hyper-button exits. After you expand the node, the hyper-button exits also appear in the detail area.
4. Expand the UnSecured node to view and select applications (interactive and batch) and hyper-button exits.

   After you expand the node, the hyper-button exits also appear in the detail area.
5. In the Create with region, select the **Run Security** option.

   When you select this option, the grid shows an **N** in the Run column for each object.
6. Click **Find**.
7. Drag exits one at a time from the UnSecured node to the Secured node.

   The exits that you dragged now appear under the Secured node. The grid reflects the security that you set for these exits. This security prevents the user that you entered from using the exit.

Note: Hyper Exit security with Run=N for *ALL objects is ignored on the web client for Tools Release 8.97 and earlier releases.

Removing Hyper Exit Security

Enter **P00950** in the Fast Path.

1. On the Work With User/Role Security form, select the **Form** menu, **Set Up Security**, **Hyper Exit**.
2. Complete these fields and click **Find**:
   - User / Role

     Enter a complete user or role ID, which includes *PUBLIC but not wildcards.
   - Application

     View security for a specific application. Enter `*ALL` to display *all* applications.

     Current security settings for the user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as interactive and batch. After you expand the node, the secured hyper-button exits also appear in the detail area.

3. Perform one of these steps:
   - Under the Secured node, select a hyper exit and click **Delete**.
   - Under the Secured node, drag a hyper exit from the Secured node to the UnSecured node.
   - On the Row menu, select **Remove All** to move all hyper exits from the Secured node to the UnSecured node.

Managing Exclusive Application Security

This section contains the following topics:

- Add exclusive application security.
- Remove exclusive application access.

Understanding Exclusive Application Security

Exclusive application security enables you to grant access to otherwise secured information through one exclusive application. For example, assume that you use row security to secure a user from seeing a range of salary information; however, the user needs to run a report for payroll that includes that salary information. You can grant access to the report, including the salary information, using exclusive application security. EnterpriseOne continues to secure the user from all other applications in which that salary information might appear.

Adding Exclusive Application Security

Enter P00950 in the Fast Path.

1. On the Work With User/Role Security form, select the **Form** menu, **Set Up Security**, **Exclusive App**.
2. On the Exclusive Application Security form, complete the User / Role field.

   Enter a complete user or role, which includes *PUBLIC but not wildcards.
3. Complete these fields in the detail area:
   - Object Name

     Enter the name of the exclusive application for which you want to allow access (the security). For example, to change the security for a user of the Vocabulary Overrides application, enter P9220 in this field.
   - Run Application
4. Click **OK** to save the information.

Removing Exclusive Application Access

Enter P00950 in the Fast Path.

1. On the Work With User/Role Security form, select the **Form** menu, **Set Up Security**, **Exclusive App**.
2. On **the** Exclusive Application Security form, complete the User / Role field and click Find.

> **Note:** If you accessed the Exclusive Application Security form from a specific record in the Work With User/Role Security form, the user or role associated with the security record appears in the User/Role field by default.

3. Highlight the security records in the grid and click **Delete**.
4. On the Confirm Delete message form, click **OK**.
5. Click **OK** when you finish deleting exclusive application security.

   If you do not click OK after you delete the security records, JD Edwards EnterpriseOne does not save the deletion.

Managing External Calls Security

This section contains the following topics:

- *Understanding External Call Security*
- *Adding External Call Security*
- *Removing External Call Security*

Understanding External Call Security

In EnterpriseOne, certain applications exist that are not internal to EnterpriseOne; they are standalone executables. For example, the Report Design Aid, which resides on the Cross Application Development Tools menu (GH902), is a standalone application. You can also call this application externally using the RDA.exe. By default, this file resides in the `\E810\SYSTEM\Bin32` directory.

Adding External Call Security

Enter `P00950` in the Fast Path.

1. On the Work With User/Role Security form, select the **Form** menu, **Set Up Security**, **External Calls**.
2. On the External Calls Security form, complete these fields and click **Find**:
   - User / Role

     Enter a complete user or group ID, which includes *PUBLIC but not wildcards.
   - Executable

     Enter the name of the external application, such as **debugger.exe.** When you enter information into this field, the software searches only for the indicated application.

     Current security settings for that user or group appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as debugger.exe.
3. In the Create with region, select the **Run Security** option.
4. Complete one of these steps:
   - Drag applications from the UnSecured node to the Secured node.

- To move all applications to the Secured node, select **All Objects** from the Row menu.

  The external call applications now appear under the Secured node and have the appropriate security.

  For example, to set run security on the Business Function Design application, select the Run Security option and then drag the Business Function Design node from the UnSecured node to the Secured node. The detail area reflects the run security that you set for this application, which means that the user you entered could *not* run the Business Function Design application.

5. To change the security on an item, select the item under the Secured node, select the **Run Security** option, and then, from the Row menu, select **Revise Security**.

   In the grid, the value in the Run field changes accordingly.

Removing External Call Security

Enter `P00950` in the Fast Path.

1. On the Work With User/Role Security form, select the **Form** menu, **Set Up Security**, **External Calls**.
2. On the External Calls Security form, complete these fields and click Find:
   - User / Role

     Enter a complete user or group ID, which includes ***PUBLIC** but not wildcards.
   - Executable

     Enter the name of the external application, such as **debugger.exe.** When you enter information into this field, the software searches only for the indicated application.

     Current security settings for that user or group appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as debugger.exe.
3. Perform one of these steps:
   - Under the Secured node, select an application and click Delete.
   - Under the Secured node, drag an application from the Secured node to the UnSecured node.
   - On the Row menu, select Remove All to move *all* applications from the Secured node to the UnSecured node.

Managing Miscellaneous Security

This section contains the following topics:

- *Understanding Read/Write Reports Security*
- *Managing Miscellaneous Security Features*

Understanding Read/Write Reports Security

EnterpriseOne enables administrators to prevent specific users and roles from running reports that update EnterpriseOne database tables (read/write reports). Administrators can assign users to a user profile called No Update Report Creation User (NUR), which restricts users to running only read-only reports. When an NUR user runs a report,

EnterpriseOne prevents the report from making table input/output (I/O) calls to databases that can affect business data. Users assigned to this profile can create and run read-only reports, but are restricted from creating or running existing UR reports. NUR users can copy existing UR reports and run the copied report, although the software disables the report's ability to change business data and displays a warning that the copied report cannot be updated. NUR users can edit NUR reports in Report Design Aid, but are prevented from even opening existing UR reports in RDA.

Managing Miscellaneous Security Features

Enter `P00950` in the Fast Path.

1. On the Work With User/Role Security form, select the **Form** menu, **Set Up Security**, **Misc Security**.
2. On the Miscellaneous Security form, complete the User / Role field and click **Find**.

   Enter a complete user or role, which includes *PUBLIC but not wildcards.
3. To change Read-Only Report security, select one of these options:
   - Read / Write
   - Read Only
4. To change Workflow Status Monitoring security, select one of these options:
   - Secured

     Prevents users from viewing or administering workflow.
   - View

     Allows users to view workflow but prevents them from making changes.
   - Full

     Allows users to view and administer workflow.
5. Click **OK** to accept the changes.

Managing Push Button, Link, and Image Security

This section contains the following topics:

- *Understanding Push Button, Link, and Image Security*
- *Adding Push Button, Link, and Image Security*
- *Removing Push Button, Link, and Image Security*

Note: Push button, link, and image security is enforced only for interactive applications in the JD Edwards EnterpriseOne HTML client and the Portal. It is not supported on the Microsoft Windows client.

Understanding Push Button, Link, and Image Security

EnterpriseOne enables you to secure users from using or viewing push button, link, and image controls. You can secure users from using a control but still allow them to view it. Or you can prevent users from both using and viewing a control.

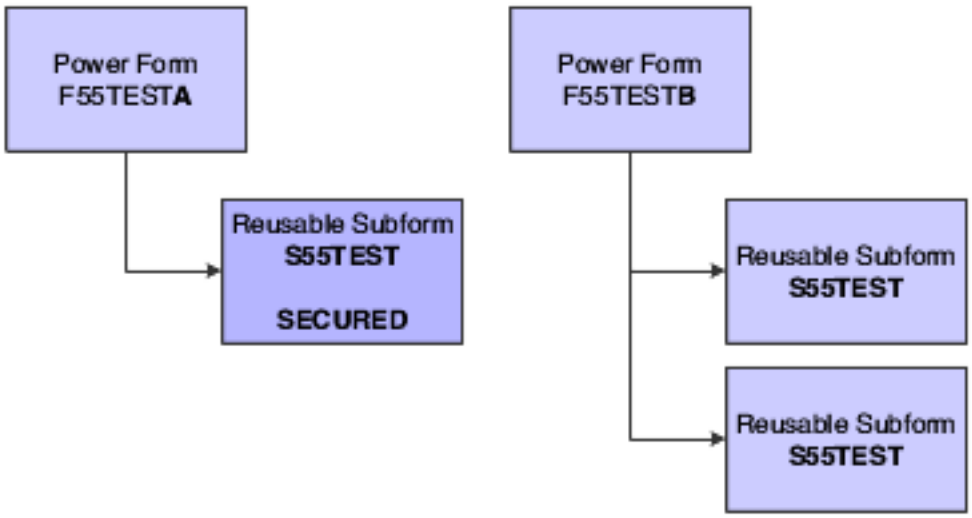
Note: In EnterpriseOne forms, static text and text boxes can be made into links. However, you can only apply security to static text links, not to text box links.

Security Workbench displays the objects that you want to secure in a hierarchical tree structure that contains nodes for each application, application version, and form. Security Workbench only displays the forms that contain push button, link, and image controls. You can secure an individual control by dragging the control from the UnSecured node to the Secured node. In addition, you can secure all controls—push buttons, links, or images—on a form by dragging the form node to the Secured node. You can perform the same action on applications and application versions. For example, to secure all the links within an entire application, you drag the application from the UnSecured node to the Secured node to secure all the links in every form within the application as well as within any versions of the application. If you drag an application version node to the Secured node, only the links in that application version are secured.

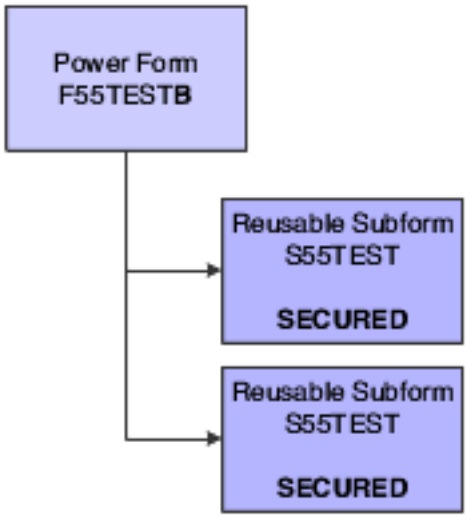
Note: For security purposes JD Edwards EnterpriseOne does not allow cross site scripting to be executed.

Push Button, Link, and Image Security on Subforms

You can secure push buttons, links, and images on both embedded and reusable subforms in EnterpriseOne. If you secure controls on an embedded subform, only the controls within that subform are secured. For reusable subforms, the behavior of the security depends upon the context in which the reusable subforms are used in power forms. If you apply security to a reusable subform under a power form, then only the controls in that reusable subform for that particular power form are secured, even if the reusable subform is used by another power form, as shown in this diagram:



However, if you apply security to a reusable subform under a power form, and that subform is reused in the same power form, the security is applied to both subforms, as shown in this diagram:



Because security functions differently on embedded subforms than it does on reusable subforms, Security Workbench provides a way for you to distinguish between the two forms. To make this distinction, the tree structure in Security Workbench displays the embedded subform using its form ID, and it displays the reusable subform using its form title.

Adding Push Button, Link, and Image Security

Enter `P00950` in the Fast Path.

1. On Work With User/Role Security, select the **Form** menu, **Set Up Security**, and then select the **Push Button**, **Link**, or **Image** menu, depending on the type of object that you want to secure.
2. Complete the User / Role field and click **Find**.
   Enter a complete user or role, which includes *PUBLIC.
3. In the Display UnSecured Items region, complete the appropriate fields and then click **Find**:
   - Application
     Enter an interactive application name, such as `P01012`. Enter `*ALL` to display all applications.
     > **Note:** Batch applications are not supported.
   - Version
     You can enter a particular version of the application that you entered in the Application field. If you leave this field blank, Security Workbench displays all unsecured versions associated with the application in the UnSecured node.
   - Product Code
     Enter a product code to display all applications, versions, and forms associated with a particular product code. This field does not work in conjunction with the Application and Version fields.

   The search results appear under the UnSecured node.
4. Expand the UnSecured node to view the individual applications or versions, and the forms associated with each.
   Only the forms that contain controls are displayed.

5. Under the Create with region, select the type of security that you want to apply:
   - View

     This option prevents the user from using and viewing the control.
   - Enable

     This option prevents the user from using the control. However, the control is still visible.
6. Use one of these actions to secure the items:
   - Drag items from the UnSecured node to the Secured node.
   - From the Row menu, select **All Objects** to move all applications to the Secured node.

     The system displays the items under the Secured node that have the appropriate security. You can view the security for each item in the grid.

Removing Push Button, Link, and Image Security

Enter `P00950` in the Fast Path.

1. On the Work with User/Role Security form, select the **Form** menu, **Set Up Security**, and then either the **Push Button**, **Link**, or **Image** menu.
2. Enter a user or role ID from which you want to remove the security in the User / Role field.

   Enter a complete user or role, which includes *PUBLIC but not wildcards.
3. Click **Find**.

   Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications. After you expand the node, the applications that are secured also appear in the detail area.
4. Perform one of these steps:
   - Under the Secured node, select an application or application version and click **Delete**.
   - Under the Secured node, drag an application or application version from the Secured node to the UnSecured node.
   - On the Row menu, select **Remove All** to move *all* items from the Secured node to the UnSecured node.

Managing Text Block Control and Chart Control Security

This section contains the following topics:

- *Understanding Text Block Control and Chart Control Security*
- *Reviewing Current Text Block Control and Chart Control Security Settings*
- *Adding Text Block Control and Chart Control Security*
- *Removing Text Block Control and Chart Control Security*

Understanding Text Block Control and Chart Control Security

JD Edwards EnterpriseOne enables you to secure users from using or viewing text block and chart controls. You can secure users from using a control but still allow them to view it. Or you can prevent users from both using and viewing a control.

In JD Edwards EnterpriseOne, a text block or chart control can have separate segments that contain links to other objects. You cannot secure these individual segments of a control. When you secure a text block or chart control, security is applied to the entire control.

Note: *"Understanding Text Block Controls" in the JD Edwards EnterpriseOne Tools Form Design Aid Guide* .

Reviewing Current Text Block Control and Chart Control Security Settings

Enter `P00950` in the Fast Path.

1. On the Work With User/Role Security form, select the **Form** menu, **Set Up Security** and then select the **Text Block Control** or **Chart Control** menu.
2. Enter the user or role ID in the User / Role field and click **Find**.

   You can enter `*PUBLIC` but not wildcards.

   The system displays the control security settings for the user or role under the Secured node in the tree.
3. To see if control security is applied to a particular application, version, or form, complete a combination of these fields in the Display UnSecured Items region, and then click **Find**:

   - Application

     Enter an application name, such as `P01012`.
   - Version

     Enter a version of the application entered in the Application field to see if control security is applied to the version.
   - Form Name

     Enter a form name, such as `W0101G`.
4. Expand the Secured node and click a secured item to view the current security settings for the user or role in the detail area.

Adding Text Block Control and Chart Control Security

Enter `P00950` in the Fast Path.

1. On Work With User/Role Security, select the **Form** menu, **Set Up Security**, and then select the **Text Block Control** or **Chart Control** menu, depending on the type of control that you want to secure.

2. Complete the User / Role field and click **Find**.
   Enter a complete user or role, which includes *PUBLIC.
3. In the Display UnSecured Items region, complete the appropriate fields and then click **Find**:
   - Application
     Enter an interactive application name, such as `P01012`. Enter `*ALL` to display all applications.
     > **Note:** Batch applications are not supported.
   - Version
     You can enter a particular version of the application that you entered in the Application field. If you leave this field blank, Security Workbench displays all unsecured versions associated with the application in the UnSecured node.
   - Product Code
     Enter a product code to display all applications, versions, and forms associated with a particular product code. This field does not work in conjunction with the Application and Version fields.

   The search results appear under the UnSecured node.
4. Expand the UnSecured node to view the individual applications or versions, and the forms associated with each.
   Only the forms that contain controls are displayed.
5. Under the Create with region, select the type of security that you want to apply:
   - View
     This option prevents the user from using and viewing the control.
   - Enable
     This option prevents the user from using the control. However, the control is still visible.
6. Use one of these actions to secure the items:
   - Drag the text block or chart control from the UnSecured node to the Secured node.
   - Select the control that you want to secure and then select **Secure Selected** from the Row menu.
   - From the Row menu, select **All Objects** to move all applications to the Secured node.
     The system displays the items under the Secured node that have the appropriate security. You can view the security for each item in the grid.

Removing Text Block Control and Chart Control Security

Enter **P00950** in the Fast Path.

1. On the Work with User/Role Security form, select the **Form** menu, **Set Up Security**, and then select the **Text Block Control** or **Chart Control** menu.
2. Enter a user or role ID from which you want to remove the security in the User / Role field.
   Enter a complete user or role, which includes *PUBLIC but not wildcards.
3. Click **Find**.

Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications. After you expand the node, the applications that are secured also appear in the detail area.

4. Perform one of these steps:
   - Under the Secured node, select an application or application version and click **Delete**.
   - Under the Secured node, drag an application or application version from the Secured node to the UnSecured node.
   - On the Row menu, select **Remove All** to move *all* items from the Secured node to the UnSecured node.

Managing Media Object Security

This section contains the following topics:

- *Understanding Media Object Security*
- *Reviewing the Media Object Security Settings*
- *Adding Media Object Security*
- *Removing Media Object Security*

Understanding Media Object Security

JD Edwards EnterpriseOne enables you to secure users from adding, changing, deleting, or viewing media objects within interactive applications, forms, or application versions. You can apply media object security to ensure that media object attachments cannot be modified or tampered with after they have been added.

As of Tools Release 9.2.6, JD Edwards EnterpriseOne enables you to secure users from adding, changing, deleting, or viewing media objects through AIS REST APIs or Orchestrations based on the media object structure being accessed in the APIs.

If you apply view security to media object attachments, Security Workbench automatically prevents the user from adding, deleting, or changing media objects. If you apply change security to media object attachments, Security Workbench automatically prevents the user from deleting the media object.

Media object security enables you to use media object attachments as a mechanism for recording justifications for transactions and for legal purposes. For example, your company may have a business process that requires clerks to use media object attachments to document the reason or justification for adjusting a price on an item in a transaction. In this case, you would allow the clerks to add and view media object attachments in an application, but secure them from deleting or modifying them. In addition, this type of security prevents users from modifying or deleting attachments that others have added. As a result, the media object attachments provide secured information about previous transactions. This information can be reviewed by interested parties for legal or other purposes.

> **Note:** Media object security is enforced only in interactive applications on the JD Edwards EnterpriseOne web client and the Portal. It is not supported on the Microsoft Windows client. Also, media object system functions enforce media object security in the web client. When running applications that have media object security applied to them, the system logs the security information for the system functions in the web client debug log file.

Reviewing the Media Object Security Settings

To review the Media Object Security Settings for applications:

1. Enter `P00950` in the Fast Path.
2. On the Work With User/Role Security form, select the **Form** menu, **Media Object**, **Applications**.
3. On the Media Object Security form, enter the user or role ID in the User / Role field and click **Find**.
   You can enter `*PUBLIC` but not wildcards.
   The system displays current media object security settings for the user or role under the Secured node in the tree.
4. To see if a media object security is applied to a particular application, version, or form, complete a combination of these fields in the Display UnSecured Items region, and then click **Find**:
   - Application
     Enter an application name, such as `P01012`.
   - Version
     Enter a version of the application entered in the Application field to see if media object security is applied to the version.
   - Form Name
     Enter a form name, such as `W0101G`.
5. Expand the Secured node and click a secured item to view the current security settings for the user or role in the detail area.

(9.2 Update 6) To review the Media Object Security Settings for services:

1. Enter `P00950` in the Fast Path.
2. On the Work With User/Role Security form, select the **Form** menu, **Media Object**, **Services**.
3. On the Media Object Security form, enter the user or role ID in the User / Role field and click **Find**.
   You can enter `*PUBLIC` but not wildcards.
   The system displays current media object security settings for the user or role under the Secured node in the tree.
4. To see if a media object security is applied to a particular service,enter the GT structure name in the Service field and click **Find**.
5. Expand the Secured node and click a secured item to view the current security settings for the user or role in the detail area.

Adding Media Object Security For Applications

1. Enter `P00950` in the Fast Path.
2. On the Work With User/Role Security form, select the **Form** menu, **Media Object**, **Applications**.
3. On the Media Object Security form, enter the user or role ID in the User / Role field and click **Find**.
   You can enter `*PUBLIC` but not wildcards.
   Current media object security settings for the user or role appear under the Secured node in the tree.

4. To find the applications, versions, or forms to which you want to apply media object security, complete any of these fields in the Display UnSecured Items region, and then click **Find**:
   - Application

     Enter an application name, such as `P01012`. Enter `*ALL` to display all applications.
   - Version

     Enter a version of the application you entered in the Application field. If you leave this field blank, all versions associated with the application will appear in the UnSecured node.
   - Product Code
5. Expand the Unsecured node to view individual applications, versions, and forms in the detail area.
6. In the Create with region, select any of these options:
   - Change
   - Add
   - Delete
   - View

   > **Note:** If you apply view security to media object attachments, Security Workbench automatically prevents the user from adding, deleting, or changing media objects. If you apply change security to media object attachments, Security Workbench automatically prevents the user from deleting the media object.
7. To secure the media objects on an application, application version, or form, perform one of these steps:
   - Drag the application, version, or form from the UnSecured node to the Secured node.
   - From the Row menu, select **All Objects** to move all items to the Secured node.
   - From the Row menu, select **Secure to All** to move all objects beneath the UnSecured node to the Secured node.

     For example, to set delete security, select the **Delete** option. Next, drag the application from the UnSecured node to the Secured node. The detail area will reflect the media object security that you set for this application.

     The applications or forms now appear under the Secured node, and they have the appropriate media object security.

Adding Media Object Security For Services (9.2 Update 6)

> **Note:** Any calls to AIS Services through jderest/file or jderest/v2/file endpoint will comply with these security settings. Also, any Attachment step within an orchestration will comply with these security settings.

1. Enter `P00950` in the Fast Path.
2. On the Work With User/Role Security form, select the **Form** menu, **Media Object**, **Services**.

3. On the Media Object Security form, enter the user or role ID in the User / Role field and click **Find**.

   You can enter `*PUBLIC` but not wildcards.

   Current media object security settings for the user or role appear under the Secured node in the tree.
4. To find the services to which you want to apply media object security, complete any of these fields in the Display Secured Items or Display UnSecured Items region, and then click **Find**:
   - Services

     Enter the service (GT Structure).
   - Product Code
5. Expand the Unsecured node to view individual applications, versions, and forms in the detail area.
6. In the Create with region, select any of these options:
   - Change
   - Add
   - Delete
   - View
7. To secure the media objects on an application, application version, or form, perform one of these steps:
   - Drag the application, version, or form from the UnSecured node to the Secured node.
   - From the Row menu, select **All Objects** to move all items to the Secured node.
   - From the Row menu, select **Secure to All** to move all objects beneath the UnSecured node to the Secured node.

     For example, to set delete security, select the **Delete** option. Next, drag the application from the UnSecured node to the Secured node. The detail area will reflect the media object security that you set for this application.

     The services (GT Structures) now appear under the Secured node, and they have the appropriate media object security.

Removing Media Object Security

Enter `P00950` in the Fast Path.

1. On the Work With User/Role Security form, select the **Form** menu, **Media Object** and then select **Applications** or **Services**.
2. In the User / Role field, enter a user or role ID from which you want to remove media object security.

   Enter a complete user or role, which includes *PUBLIC but not wildcards.
3. Click **Find**.

   Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications. After you expand the node, the applications that are secured also appear in the detail area.
4. Perform one of these steps:
   - Under the Secured node, select an application or application version and click **Delete**.

- Under the Secured node, drag the item that is secured from the Secured node to the UnSecured node.
- On the Row menu, select **Remove All** to move *all* items from the Secured node to the UnSecured node.

Managing Application Query Security

This section contains the following topics:

Understanding Application Query Security

Application Query Security prevents users from performing searches if they have not entered search criteria in the form filter fields or QBE fields. If users try to perform a search without entering search criteria, they receive an error or warning message that alerts them that their search has been suppressed. If users enter search criteria, then the search functionality will proceed.

Note: *Click here to view a recording of this feature.*

Setting Up Application Query Security for Applications

You set up application query security at the form level for all users.

Enter `P00950` in the Fast Path.

1. On Work with User/Role Security, select the **Form** menu, **Set Up Security,** and then click **App Query Security**.

   The Work with Application Query Security form displays.
2. On Work with Application Query Security, select the **Form** menu, and then select **Add Application**.

   The Setup Application Query Security form displays.
3. Select **Application**.
4. In the Application Name field, enter the application name to which you are adding query security, or click the **Search** button and select an application from the Interactive Application Search and Select form.

5. In the Form Name field, enter the form name to which you are adding query security, or click the **Search** button and select a form from the Interactive Application Search and Select form.

   For example, if you enter `W01012B` in the Form Name field, then the options you assign for the query security will apply to the Work With Address Book (W01012B) form.
6. Select one of the following Field Entry Requirements:
   - At Least One Form Filter or QBE Field

     Select this option if users must enter search criteria into at least one filter field on the form or QBE column.
   - Configured Fields

     Select this option to select one or more required form filter fields or QBE fields for the form.
7. Select one of the following Message Types:
   - Error

     Select this option if you want an error message to pop up when users try to execute a query that does not satisfy the Field Entry Requirements specified previously.
   - Warning

     Select this option if you want a warning message to pop up when users try to execute a query that does not satisfy the Field Entry Requirements specified previously.
8. Click **OK**.

Setting Up DataBrowser Query Security

You set up databrowser query security records if you want to secure users from entering wide open queries from the Data Browser. Similar to Application Query Security, you can specify required filter fields and QBE columns the user must enter when querying via the Data Browser.

Use these steps to set up DataBrowser query security:

1. Access your web client application.
2. In the Fast Path field, type `P00950`.

   The Work with User/Role Security form displays.
3. From the Form menu, select **Set Up Security**, and then **App Query Security**.

   The Work with Application Query Security form displays.
4. From the Form menu, click **Add Application**.

   The Setup Application Query Security form displays.
5. From the Form menu, click **Add Application**, and then select **Databrowser**.

   Notice that DATABROWSE already displays in the Application Name field, and the databrowser options display.
   - At Least One Form Filter Field or QBE Field

     Select this option if users must enter search criteria into at least one filter field on the form or QBE column.
   - Configured Fields

Select this option to select one or more required form filter fields or QBE fields for the form.

6. Select one of the following Message Types:
   - Error

     Select this option if you want an error message to pop up when users try to execute a query that does not satisfy the Field Entry Requirements specified previously.
   - Warning

     Select this option if you want a warning message to pop up when users try to execute a query that does not satisfy the Field Entry Requirements specified previously.
7. Click **OK**.

Selecting Error or Warning Messages

You can opt for users to see an error or warning message when they try to search for data without entering search criteria on a form.

Use these steps to select error or warning messages:

1. Access the EnterpriseOne web client.
2. In the Fast Path field, type `P00950`.

   The Work with User/Role Security form displays.
3. From the Form menu, select **Set Up Security**, and then **App Query Security**.

   The Work with Application Query Security form displays. Any query security instances that have already been set up display in the grid.
4. From the grid, select the existing record, and then click **Select**.

   The Setup Application Query Security form displays with all of the application and form name query security information.
5. Select one of the following Message Types:
   - Error

     Select this option if you want an error message to pop up when users try to execute a query that does not satisfy the Field Entry Requirements specified above.
   - Warning

     Select this option if you want a warning message to pop up when users try to execute a query that does not satisfy the Field Entry Requirements specified previously.
6. Click **OK**.

Finding Existing Query Security Records

Use these steps to find existing query security records:

1. Access your web client application.
2. In the Fast Path field, type `P00950`.

The Work with User/Role Security form displays.

3. From the Form menu, click **Set Up Security**, and then click **App Query Security**.

   The Work with Application Query Security form displays. Any query security instances that have already been set up display in the grid.
4. Select Application Secured to view the application that have query security, or select Excluded Users to view the list of users excluded from the query security.

   For each Application Query Security record, you can define one or more users that are excluded from the security. These users are called Excluded Users. See the *Excluding Users* section of this document for details.
5. Click **Close**.

Editing Existing Query Security Records

You can edit records with existing information like Field Entry Requirements, Error type and enable and disable security records.

Use these steps to edit an existing query security record:

1. Access your web client application.
2. In the Fast Path field, type `P00950`.

   The Work with User/Role Security form displays.
3. From the Form menu, select **Set Up Security**, and then **App Query Security**.

   The Work with Application Query Security form displays. Any query security instances that have already been set up display in the grid.
4. Click **Find**.
5. From the grid, select the existing query security record, and then click **Select**.

   The Setup Application Query Security form displays with all of the application and form name query security information.
6. Select one of the following Field Entry Requirements:
   - Form Filter Field

     Select this option if users must enter search criteria into at least one filter field on the form or QBE column.
   - QBE Fields

     Select this option if you want users to enter search criteria into a QBE field on a grid.
7. Select one of the following Message Types:
   - Error

     Select this option if you want an error message to pop up when users try to execute a query that does not satisfy the Field Entry Requirements specified above.
   - Warning

     Select this option if you want a warning message to pop up when users try to execute a query that does not satisfy the Field Entry Requirements specified previously.
8. Click **OK**.

Deleting Query Security Records

Deleting a query security records removes it from EnterpriseOne.

Use these steps to delete a query security record:

1. Access your web client application.
2. In the Fast Path field, type `P00950`.

   The Work with User/Role Security form displays.
3. From the Form menu, select **Set Up Security**, and then **App Query Security**.

   The Work with Application Query Security form displays. Any query security instances that have already been set up display in the grid.
4. From the grid, select the existing record, and then click **Delete**.

   A dialog box displays that says, "Are you sure you want to delete the selected item?"
5. Click **OK**.

Enabling or Disabling Query Security Records

You can set up an Application Query Security record and enable or disable it at a different time. When you disable an Application Query Security record, the record will not be enforced on the users using the application.

Use these steps to enable or disable query security records:

1. Access your web client application.
2. In the Fast Path field, type `P00950`.

   The Work with User/Role Security form displays.
3. From the Form menu, select **Set Up Security**, and then **App Query Security**.

   The Work with Application Query Security form displays. Any query security instances that have already been set up display in the grid.
4. From the grid, select the existing record, and then click **Select**.

   The Setup Application Query Security form displays with all of the application and form name query security information.
5. Select one of the following options:

   - Enable

     Select this option if you want application query security to be turned on for the application you are editing.
   - Disable

     Select this option if you want application query security to be turned off for the application you are editing.
6. Click **OK**.

Excluding Users

Application Query Security is applied to all users (*PUBLIC), which encompasses all users. Some users may need to perform an open ended fetch for a particular reason. Therefore, some users need to be excluded from the application query security. The Exclude Users form enables you to exclude one or more users from the application security record.

Use these steps to exclude users:

1. Access your web client application.
2. In the Fast Path field, type `P00950`.

   The Work with User/Role Security form displays. Any query security instances that have already been set up display in the grid.
3. From the Form menu, select **Set Up Security**, and then **App Query Security**.

   The Work with Application Query Security form displays. Any query security instances that have already been set up display in the grid.
4. From the grid, select the existing record, and then click the **Row** exit.
5. Click **Exclude Users**.

   The Exclude Users form displays.
6. In the User ID field, enter the ID of the user you want to exclude from the Application Query Security you have set up for the record you selected.
7. Click **OK**.

Configuring Error Messages Using Data Dictionary Items

You can configure the custom error message by using the following Data Dictionary Items. This ability enables you to add custom messages using Glossary Overrides.

- POFERR – Applications Query Security Error
- POFWAR - Applications Query Security Warning

Use these steps to configure error messages using data dictionary items:

1. Access your web client application.
2. In the Fast Path field, type `DD`.
3. Click **Work with Data Dictionary Items**.
4. In the Alias field of the QBE line, enter `POFERR`.
5. Click **Find**, and then select the DD Item.

   By default it comes with default error message in item glossary.
6. From the Row menu, select **Glossary Overrides**.
7. Click **Add**.
8. Enter the appropriate information, and then click **OK** to save.
9. In the Work with Data Dictionary Items form click **Find** and select the entered record.
10. Click **Select** to enter the custom message.
11. Enter the text in the attachment and click on **OK** to save the data.

Configured Fields Option

The Configured Fields option enables you to select one or more specific form filter fields, QBE fields, or both for the required search criteria.

Use these steps to configure fields:

1. Follow the steps for Setting Up Application Query Security for Applications, making sure to select the Configured Fields option.
2. From the Tools menu, select **Configured Fields**.

   The available form filter fields and QBE fields display.
3. Select the required fields for the search value, and then click **Save**.

Managing Data Browser Security

This section contains the following topics:

- *Understanding Data Browser Security*
- *Adding Data Browser Security*
- *Adding Data Browser Security through the UDO View Security Form (Alternative Method)*
- *Removing Data Browser Security*

Understanding Data Browser Security

Data Browser security enables you to grant permission to users, roles, or *PUBLIC to access the Data Browser application. There are two levels of Data Browser security that you can assign to users. The first level grants access to the Data Browser, which users can use to perform public or personal queries. After you grant this access, you can grant an additional level of security that allows Data Browser users to select a particular table or business view that they wish to query.

You can also use the Copy feature in Security Workbench to copy Data Browser security from one user or role to another.

Note: *"Viewing the Data in Tables and Business Views" in the JD Edwards EnterpriseOne Tools Foundation Guide* .

Adding Data Browser Security

Enter **P00950** in the Fast Path.

1. On the Work With User/Role Security form, select the **Form** menu, **Set Up Security**, **Data Browser**.
2. On the Data Browser Security form, enter the user or role ID in the User / Role field and click **Find**.

   You can enter `*PUBLIC` but not wildcards.

3. In the Data Browser hierarchical security permissions region, select one or both of these options, depending on the level of security that you want to grant:
   - Allow access to launch Data Browser.

     This option gives users access to the Data Browser, which they can use to perform personal or public queries.
   - Allow access to Search and Select for Tables or Business View Queries.

     This option gives users the ability to search and select the table or business view that they want to query.

     > **Note:** This option is enabled only after you select the first option.
4. Click **OK**.

> **Note:** To activate Data Browser security changes, you must use Server Manger to refresh the jdbj security cache.

Adding Data Browser Security through the UDO View Security Form (Alternative Method)

Even through the Data Browser is not related to user defined objects (UDOs), the form used to set up view security for UDOs provides an easy way to set up security for the Data Browser.

To set up Data Browser security through the Work With User Defined Object View Security form:

1. Access P00950.
2. Select the **Form** menu, **User Defined Object View**.
3. On Work With User Defined Object View Security, click the **Add** button.
4. In an empty row in the grid, complete the following fields:
   - **User/Role**. Enter a user or role for which you want to enable access to the Data Browser.
   - **Form Name**. Click the search button to locate a form or table that you want a user or role to be able to search over in the Data Browser. You can enter *ALL if you want to enable a user or role to search over all forms and tables. You can also enter a product code or reporting code if you want to limit the search to one of these items.
5. Click the **OK** button.
6. Set up additional records as necessary.

Removing Data Browser Security

You can remove Data Browser security using the Data Browser Security form or the Work With User/Role Security form. To remove security using the Data Browser Security form, clear the security check boxes for a user, role, or *PUBLIC. Using the Work With User/Role Security form, search for the security record and then delete the Data Browser security record from the grid.

Managing Published Business Services Security

This section contains the following topics:

Understanding Published Business Services Security

JD Edwards EnterpriseOne provides security to ensure that web service consumers are authenticated in the JD Edwards EnterpriseOne system and authorized to access published business services. The authentication of users of published business service users is handled by the Business Services Server and EnterpriseOne security server. After a user is authenticated by the JD Edwards EnterpriseOne security server, the system checks if the user is authorized to run a published business service by retrieving records from the JD Edwards EnterpriseOne F00950 security table, which contains all the object security records.

Note: This section discusses only the authorization of users to access published business services.

For published business services, JD Edwards EnterpriseOne uses a "secure by default" security model which means that users cannot access a published business service unless a security record exists that authorizes access. For most other objects in JD Edwards EnterpriseOne, access is granted unless otherwise secured or restricted.

You manage published business services security using Security Workbench (P00950), the application used to manage all object security in JD Edwards EnterpriseOne. In P00950, you can add, copy, modify, or delete security records for published business services. When a user tries to access or run a published business service, verification of authorization is done through an API that queries records in the F00950 security table.

As with all object security in JD Edwards EnterpriseOne, you can assign published business service security to a user, role, or *PUBLIC. You can create a security record that allows a user or role access to:

- A particular method in a published business service.
- All methods in a published business service.
- All published business services.

It is recommended that you set up security by role first. This method makes setting up published business services security easier; instead of defining security for individual users, you can define security for the role and then assign users to the appropriate roles. If an individual in a role needs a different security setup, you can assign security at the user level, which overrides the role settings.

In addition, you can create a security record that disallows access to a published business service. Typically, there is no need to add security records that disallow access because by default, access to published business services is not allowed. However, creating a security record that disallows access can be an efficient method to set up published

business services security. For example, to allow a role access to all but a small subset of published business services, you can:

- Enter `*ALL` in the fields for the published business service and published business service method to create a security record that allows the role access to all published business services.
- Create security records for the same role that disallows access to a subset of published business services.

Inherited Security

When creating a published business service, a developer can configure it to pass its context to any published business service that it calls. In this configuration, authorization for the called published business service is inherited; that is, if the calling business service is authorized, then the called business service is authorized as well. In this scenario, the system does not check the security for the called business service.

However, it is possible (though not supported) to configure a published business service so that it does not pass its context to another business service. In this scenario, the security or authorization for the called published business service is not inherited. Even if a user is authorized to access the calling or parent business service, the system also checks if access to the called business service is allowed. As a result, if there is not a security record that allows access to the called business service, the system will produce an exception or error, denying access to the called business service.

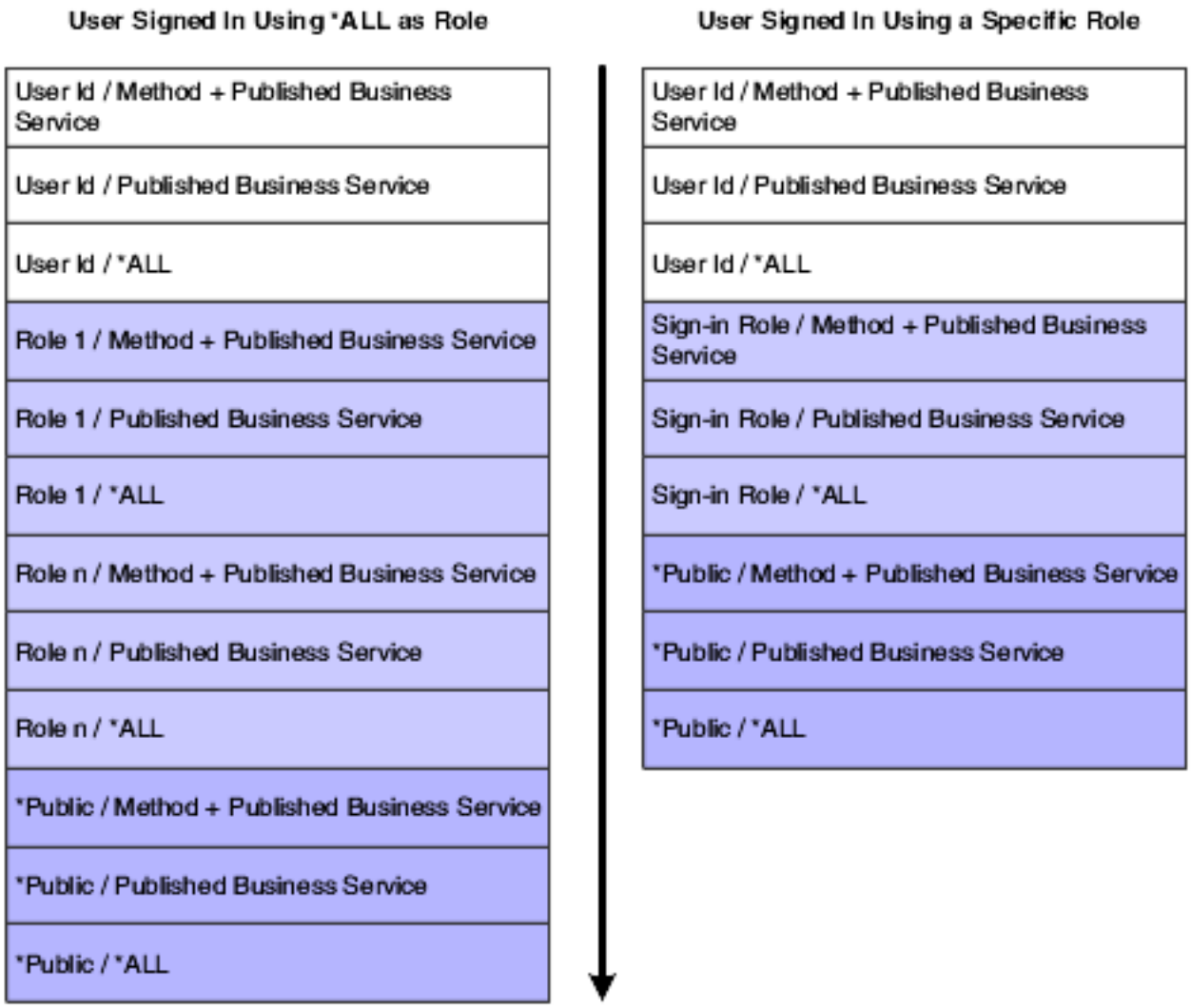
How JD Edwards EnterpriseOne Checks Published Business Services Security

JD Edwards EnterpriseOne checks security for published business services in the same sequence that it checks security for all other JD Edwards EnterpriseOne objects—first by user, then role, and finally *PUBLIC. The system applies the first security record found. In addition, for the user, role, and *PUBLIC, the system checks for published business services security in this sequence:

- Published business service + method.
- Published business service.
- *ALL.

Note: Using *ALL to set up object security in Security Workbench is not related to the *ALL functionality that is used to sign into JD Edwards EnterpriseOne. *ALL in Security Workbench enables you to assign a user, role, or *PUBLIC to all objects of a particular type. *ALL during sign-in enables users to sign into JD Edwards EnterpriseOne with all the roles that have been assigned to them.

This illustration shows how the system checks for published business services security for a user signed in with *ALL and a user signed in with a specific role:



If a user is assigned to multiple roles and signs in as *ALL, the system uses role sequencing to determine which security record is used. A system administrator sets up role sequencing when setting up user and role profiles.

See *Sequencing Roles*.

Published Business Services Security Log Information

The log file provides administrators with information that you can use for troubleshooting business service security without revealing details that could possibly create a gap in the security.

When a web service attempts to access a published business service in JD Edwards EnterpriseOne, the system records the authorization information in the log file. If the logging level is set to "Debug," the log file records whether authorization was granted or denied. If the log level is set to "Severe," the system only logs information if the attempt to access a web service fails. This is an example of the information provided in the log file:

```
Access to <method name> in <published business service name> is <granted/denied>#
 for <user name> with <role name>.
```

See Also

- *JD Edwards EnterpriseOne Tools Server Manager Guide* for information on how to view business service security log file information.
- *JD Edwards EnterpriseOne Tools Business Services Server Reference Guide* for information on how to configure JD Edwards EnterpriseOne to authenticate users of published business services.

Reviewing the Current Published Business Services Security Records

You can use the Work With User/Role Security form in P00950 to review existing published business services security records. The query by example row of the grid enables you to display all security records for published business services. You can further narrow the search by locating the records for a user, role, or a particular published business service.

In addition, you can review published business services security records by running the Security Audit Reports—Security by Object (R009501) and Security by User/Role (R009502).

See *Running a Report that Lists Published Business Service Security Records*.

Enter `P00950` in the Fast Path.

1. On the Work with User/Role Security form, enter `S` in the Security Type column and then click **Find**.
2. To narrow the search by user or role, enter a user or role in the query by example field in the User / Role column and then click **Find**.
3. To view the security records for a particular published business service, complete the query by example field at the top of the Published BSSV column and then click **Find**.

Authorizing Access to Published Business Services

In P00950, you can create security records that allow a user, role, or *PUBLIC access to:

- A particular method in a published business service.
- A published business service.
- All published business services.

Enter `P00950` in the Fast Path.

1. On Work with User/Role Security, select the **Form** menu, **Set Up Security**, **Published BSSV**.

   By default, *PUBLIC is in the User / Role field. If any records exist for *PUBLIC, those records appear in the grid.
2. On Published Business Service Security Revision, enter the user, role, or *PUBLIC to which you want to allow access to a published business service.

3. To allow access to a particular method in a published business service:
   a. On Published Business Service Security Revision, click the search button in the Published BSSV column to search for and select a published business service.
   b. On the same form, click the search button in the Published BSSV Method column to select the method that you want to allow access to.

      On Published BSSV Method, you must enter the published business service again in the Published BSSV column to see a list of all the methods for the published business service. The system displays published business services by the method that is being exposed in the published business service. A published business service that contains multiple methods will have multiple rows in the grid, one for each method.
   c. Select the row that contains the method that you want to secure and then click the **Select** button.
   d. On Published Business Service Security Revision, click the search button in the Execute Allowed column and then select **Y** to allow access to the published business service method.
4. To allow access to a published business service (including all its methods):
   a. Click the search button in the Published BSSV column to search for published business services.
   b. On Select Business Service, complete the Business Service field and click the **Find** button.
   c. Select the published business service that you want to secure and then click the **Select** button.
   d. On Published Business Service Security Revision, in the row that contains the published business service, enter `*ALL` in the Published BSSV Method column.
   e. In the same row, click the search button in the Execute Allowed column and then select **Y** to allow access to the published business service.
5. To allow access to all published business services:
   a. Enter `*ALL` in the row under the Published BSSV column.
   b. Enter `*ALL` in the row under the Published BSSV Method column.
   c. Click **OK**.
   d. In the same row, click the search button and then select Y to allow access to the published business services objects.

      By default, users are not allowed access to published business services objects in JD Edwards EnterpriseOne. However, you can select **N** to create a security override that disallows access to an object.

Adding Multiple Published Business Services Security Records at a Time

Security Workbench provides a form that you can use to add multiple published business services security records at a time.

Enter `P00950` in the Fast Path.

1. On Work with User/Role Security, select the **Form** menu, **Set Up Security**, **Published BSSV**.
2. On Published Business Service Security Revision, from the Form menu, select **Secure by Method**.
3. On the Secure by Method form, enter the user, role, or *PUBLIC for which you want to set up published business services security, and then click the **Find** button.

   The system displays published business services by the method that is being exposed in the published business service. A published business service that contains multiple methods will have multiple rows, one for each method.

4. Use the query-by-example fields at the top of the grid to refine your search. For example, if you want to set up security for all methods that perform an add or delete, you search for those methods by typing `add*` or `delete*` in the Published BSSV Method query by example field in the grid.
5. Select the check box next to the items that you want to secure.
6. Click either the **Allow Execute** or **Disallow Execute** button.
7. On Confirm Batch Secure, click **OK**.

   The system displays the number of records that were added or updated.

Deleting Published Business Services Security

To delete published business services security records, you can use the same form that you used to authorize access to published business services.

In addition to this method, you can use the Work with User/Role Security form in P00950 to delete the records in the same way that you would delete any other object security record.

See *Deleting Security on the Work With User/Role Security Form*.

Enter `P00950` in the Fast Path.

1. On Work With User/Role Security, select the **Form** menu, **Set Up Security**, **Published BSSV**.
2. On Published Business Service Security Revision, enter the user, role, or *PUBLIC from which you want to delete a published business services security record and then click **Find**.
3. Click the check box next to the each record that you want to delete and then click the **Delete** button.
4. Click **OK** to confirm the delete.

Copying Security for a User or a Role

This section contains the following topics:

- *Understanding How to Copy Security for a User or a Role*
- *Copying All Security Records for a User or a Role*
- *Copying a Single Security Record for a User or a Role*

Understanding How to Copy Security for a User or a Role

You can copy the security information for one user or role, and then use this information for another user or role. When you copy security, you can either overwrite the current security for the user or role, or you can add the new security information to the existing security information. You can also copy all of the security records for a user or role, or you can copy one security record at a time for a user or role.

Copying All Security Records for a User or a Role

1. Enter `P00950` in the Fast Path.
2. On the Work With User/Role Security form, select the **Form** menu, User Defined Object, **View**.

3. On the Work With User Defined Object View Security form, select the Form menu, and then select **Copy Security**.

   Alternatively, access Work With User Defined Object View Security (W00950UOG) from the Work with User Defined Objects application (P98220U), select Form menu and then select Copy View Security. (Release 9.2.3)
4. Select one of these options:
   - Copy and Add

     When you copy and add security settings, you do not overwrite preexisting security for user or role.
   - Copy and Replace

     When you copy and replace security settings, the software deletes the security information for a user or role, and then copies the new security information from the selected user or role.
5. Complete these fields and click **OK**:
   - From User / Role
   - To User / Role

     The system saves the security information.

Copying a Single Security Record for a User or a Role

1. Enter `P00950` in the Fast Path.
2. On the Work With User/Role Security form, select the **Form** menu, User Defined Object, **View**.
3. On the Work With User Defined Object View Security form, click Find and locate a security record.

   Alternatively, access Work With User Defined Object View Security (W00950UOG) from the Work with User Defined Objects application (P98220U) and locate a security record. (Release 9.2.3)
4. Select the security record row that you want to copy, and select the Row menu, **Copy By User /Role**.
5. Complete the To User / Role field and click **OK**.

   The system saves the security information.

Reviewing and Deleting Security Records on the Work With User/Role Security Form

This section contains the following topics:

- *Understanding How to Review Security Records*
- *Reviewing Security on the Work With User/Role Security Form*
- *Deleting Security on the Work With User/Role Security Form*

Understanding How to Review Security Records

On the Work With User/Role Security form in P00950, you can review security records for a user or role based on security type, such as action, application, row, or any of the other types of security that can be added in P00950. The

system displays all the security records for the user or role based on the security type that you select. For example, when you search for application security records for the AP Role, the system displays all the application security records for the AP role in the application grid.

The settings for each security type are displayed as columns in the grid. The columns that appear in the grid are based on the security type that you select. For example, application security provides two different levels of security: run and install. When you search for application security records, P00950 displays only the columns for Run and Install in the grid. However, action security contains several settings, such as OK/Select, Copy, Delete, OK, and so forth. When you search for action security records, the grid displays only columns for each of these security settings. The value in the column, either Y or N, indicates whether or not each setting is secured.

In addition, you can search on all security records of a particular security type. As a result, the system displays records for every user and role with the security type that was specified. You can search on all Security Workbench records by clicking the Find button.

> **Note:** You can also review and delete security records on the form used to add a particular type of object security record, such as application, action, row, and so forth. Refer to the section on how to manage a particular type of object security for more information.

Reviewing Security on the Work With User/Role Security Form

Enter `P00950` in the Fast Path.

1. On the Work With User/Role Security form, click **Find**.
2. To search for records by user or role, complete the User/Role field and then click **Find**.
3. To narrow the search by security type, click the search button in the Security Type column to select a code and then click the **Find** button.

Deleting Security on the Work With User/Role Security Form

Enter `P00950` in the Fast Path.

1. On the Work With User/Role Security form, click **Find**.
2. To search for records by user or role, complete the User/Role field and then click **Find**.
3. To narrow the search by security type, click the search button in the Security Type column to select a code and then click the **Find** button.
4. Select a record in the grid, and then click **Delete**.
5. On Confirm Delete, click **OK**.

   Security Workbench deletes the security record and refreshes the grid.

26 Managing Security for User Defined Objects

Understanding Security for User Defined Objects

EnterpriseOne provides features for users to create custom grid formats, watchlists, queries, and other items, which are saved as user defined objects (UDOs) in EnterpriseOne. For example, if a user creates a query using the Query Manager, the query is saved as a UDO in an EnterpriseOne table. For a complete list of the types of UDOs users can create, see *UDO Types in the JD Edwards EnterpriseOne Tools Using and Approving User Defined Objects Guide.*

EnterpriseOne provides UDO security features in the Security Workbench to control:

- Which UDO features are available in EnterpriseOne.
- Who can create UDOs for their own personal use.
- Who can request to publish (or share) UDOs with other users.
- Who can modify shared UDOs created by other users.
- Who can view/use shared UDOs created by other users.

Note: *Click here to view a recording of UDO Feature, Action, and View security*.

#unique_631/unique_631_Connect_42_CEGBIJJA describes the UDO security features available in EnterpriseOne.

UDO Security Type	Description
Feature	UDO feature security activates or deactivates each UDO feature globally in the EnterpriseOne system. UDO features are secure by default; they are not available in EnterpriseOne until you activate them in the "Revise Feature Enablement" form in the Security Workbench.
Action	UDO action security determines the actions users can perform with a particular UDO feature. UDO action security is set up by UDO feature for a user, role, or *PUBLIC (all users). UDO Action security options include: • **Create**. Authorize users to create UDOs for their own personal use. • **Create and Publish**. Authorize users to create and share personal UDOs with other users. • **Create, Publish, and Modify**. Includes the preceding permissions plus the ability to modify UDOs created by other users.
View	UDO view security authorizes access to shared UDOs. You can apply UDO view security to each individual shared UDO for a user, role, or *PUBLIC. Or you can apply UDO view security to all shared UDOs of a particular UDO type. (Release 9.2.4) Beginning with Tools Release 9.2.4, as part of view security, system administrators can restrict access to the base EnterpriseOne forms so that users can access only the personalized forms and not the base forms.

UDO Security Type	Description
Content (Composite Page and Application Framework UDOs only) (Release 9.2.0.2)	UDO content security applies to Composite Page and Composite Application Framework UDOs. In addition to setting up view security for Composite Page and Composite Application Framework UDOs, you must also set up content security to authorize users to view or work with the **contents** of a Composite Page and Composite Application Framework UDO.

Understanding the Process for Sharing UDOs

When a user has permission to "Create and Publish" UDOs, the user can click the **Request to Publish** button in the UDO feature, which submits the UDO to the User Defined Object Management (P98220U) application. A designated user or system administrator uses P98220U to review UDOs before approving them. When approved, the status of the UDO changes to "Shared," at which point an administrator can set up UDO view security to grant users access to the UDO if a view security record does not already exist for UDOs of a particular type. See *Managing UDO View Security* for more information.

For more information on how to manage UDOs in P98220U, see the *JD Edwards EnterpriseOne Tools Using and Approving User Defined Objects Guide.*

Example of a UDO Security Implementation

Company A wants to implement UDO features in EnterpriseOne with the following criteria:

- Allow only supervisors in the Purchasing department to create One View reports and queries for the purpose of sharing with other users in the department.
- Allow all members of the Purchasing department to use shared UDOs created by the supervisors.
- (Release 9.2.4) Restrict access to the base forms of the Sales Order Entry application so that all members of the Sales department can only access the personalized forms.

Based on these criteria, Company A will need to perform the following tasks:

1. Activate the One View Reports Manager and Query Manager features in the "Revise Feature Enablement" form in Security Workbench. This displays these features globally in all applicable EnterpriseOne applications and forms.
2. Set up two UDO action security records: one that enables members of the Purchasing supervisors role to create and share One View reports; one that enables members of the Purchasing supervisors role to create and share queries.
3. Set up UDO view security to determine which users can use the shared One View reports and queries.
4. (Release 9.2.4) Configure base form security for the Sales Order Entry application to determine which users are restricted from accessing the base form.

Prerequisites

You must perform the following prerequisites before you can set up UDO security:

- *Define Allowed Actions for UDO Types*

- *Enable Access to UDO Security and Administration Applications*

Define Allowed Actions for UDO Types

Before setting up security for user defined objects, each UDO type (grid format, query, EnterpriseOne page, and so forth) must be set up with the proper "Allowed Actions" in the OMW Configuration System (P98230) application. This enables processing and management of user defined objects in the Web Object Management Workbench. If the allowed actions are not set up for each UDO type, you cannot set up security for user defined objects.

The *"Configuring Activity Rules" chapter in the JD Edwards EnterpriseOne Tools Object Management Workbench for the Web Guide* describes how to set up allowed actions in P98230. When setting up allowed actions for each UDO type:

- For the default project at status 21, use:

  From Project Status = 21

  To (Project Status) = 21

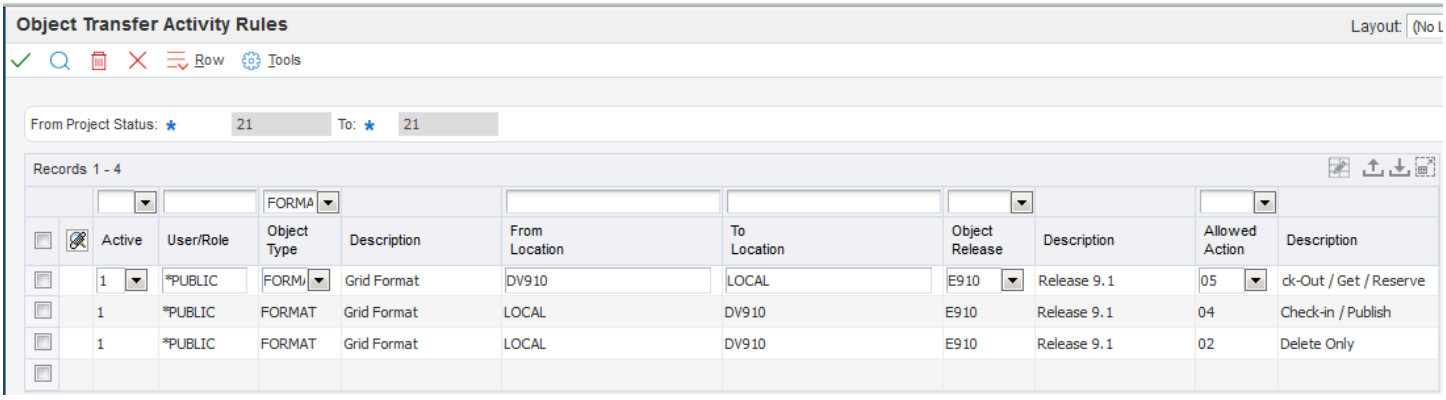
- For each UDO type, apply the following allowed actions:

  05 (Check-Out/Get/Reserve)

  02 (Delete Only)

  04 (Check-in/Publish)

The following image shows the allowed actions defined for the grid format UDO type:



Enable Access to UDO Security and Administration Applications

A security administrator must enable access to the following UDO security and administration applications before setting up UDO security:

Note: This section includes recommendations for the types of users you should authorize access to the UDO security and administration applications. You can adapt these recommendations based on your company's needs.

- **User Defined Object Management (P98220U) application**.

  This is the application for approving UDOs for sharing with other users. Oracle recommends that only an administrator, manager, or power user responsible for approving UDOs has access to this application. Typically, the approver of a shared UDO should not be the same as the user who created the UDO. Use EnterpriseOne Application security in Security Workbench to secure this application. See *Managing Application Security* in this guide.

- **Work With User Defined Object View Security application (P00950UO)**.

  This application is accessible from the User Defined Object Management (P98220U) application, the application used for approving UDOs. It is an alternative to setting up UDO view security through the Security Workbench. This form gives you the option of providing a non-Security Workbench user, or the same user who is responsible for reviewing and approving shared UDOs in P98220U, the ability to set up view security for shared UDOs. All view security records created in this application are reflected in the view security form in Security Workbench. Use Hyper Exit security in the Security Workbench to authorize access to this form from P98220U. See *Managing Hyper Exit Security* in this guide.

- **Object Management Workbench for the Web (Web OMW)**.

  This application is used to manage the life cycle of user defined objects. Oracle recommends that only developers and system administrators have access to this application.

  In addition to determining who has access to Web OMW, you have to define the actions that Web OMW users can perform, for example which users are allowed to check out and modify a UDO through the Web OMW, check in a UDO, advance a UDO to another status, and so forth. See *Configuring OMW User Roles and Allowed Actions* in this guide for more information.

In addition to the preceding applications, the Security Workbench contains forms for setting up UDO feature, action, content and view security. Only security administrators who have access to the Security Workbench have access to these forms.

Managing UDO Feature Security

UDO features are not available in EnterpriseOne until you activate the features through the Revise Feature Enablement form in Security Workbench.

To activate or deactivate UDO features:

1. On Work With User/Role Security in the Security Workbench (P00950), select the **Form** menu, **Feature Security**.
2. On Revise Feature Enablement, select the row for the UDO feature you want to activate or deactivate.
3. In the Access column, click the icon to toggle the status to active or inactive.

   If the green circle is displayed in the Access column, the feature is active. If the red square is displayed, the feature is inactive. Also, you can hover your cursor over the icon to display the status in text.

Note: When you change the status of a UDO feature to active or inactive, EnterpriseOne displays a message reminding you to clear security cache for the changes to take effect. Security cache must be cleared on the EnterpriseOne HTML Server (JAS Server). You can clear this cache using Server Manager.

Managing UDO Action Security

Set up action security for a user, role, or *PUBLIC (all users) to determine the actions users can perform when using a UDO feature. UDO action security is set up by UDO feature.

Note: You must activate the UDO feature in EnterpriseOne before setting up UDO action security. See *Managing UDO Feature Security*.

The following list describes the actions you can allow users to perform:

- **Create**. Enables users to create user defined objects for personal use. Without this permission, users can only use shared UDOs to which they have been granted access through UDO view security.
- **Create and Publish.** Enables users to create and "Request to Publish" UDOs to share UDOs with other users. "Create and Publish" security inherits the "Create" permission.

  With this permission, a user can select the "Request to Publish" button to share a UDO. However, the UDO must be approved before it can be shared with other users. For more information on how to approve UDOs in P98220U, see the *JD Edwards EnterpriseOne Tools Using and Approving User Defined Objects Guide.*
- **Modify**. Enables users to modify shared UDOs. "Modify" action security inherits "Create" and "Create and Publish" permissions.

When setting up UDO action security, remember that application security supersedes UDO action security. That is, users can only work with UDOs in applications to which they have been granted access through Security Workbench application security.

UDO action security records can be set up for a particular application, form, or application version. Or you can use *ALL (all objects) to apply action security to all applications, forms, application version in which the UDO feature exists. You also have the option to apply UDO action security to a particular EnterpriseOne product code or reporting code.

Note: If you add, modify, or delete action security, users must clear the cache in their browser for the changes to take effect.

To set up UDO Action security:

1. On Work With User/Role Security in the Security Workbench (P00950), select the **Form** menu, **User Defined Object**, **Action**.
2. On Work With User Defined Object Action Security, click the **Add** button.
3. On User Defined Object Action Security, click the search button in the Object Type field and select a UDO type.

   Note: You can ignore the DATABROWSE option. This option is for setting up Data Browser security. For more information, see *Adding Data Browser Security through the UDO View Security Form (Alternative Method)* in this guide.
4. In a row in the grid, complete the following fields to create a security record for the selected UDO type:

> **Note:** In each cell, you can click the search button to search for specific values. The search form displays only the objects that make use of the UDO feature.

- **User/Role**. Enter a specific user, role, or `*PUBLIC` (for all users).
- **App/Object Name**. Enter the application ID of the application to which you want to apply the UDO action security. Enter `*ALL` to authorize the user to perform actions in any application in which the UDO feature appears.
- **Form Name**. Enter a form ID if you want the security to apply to a specific form in the application. Or you can enter `*ALL` for all forms.
- **Version**. Enter a version if you want the security to apply to a specific version of the application. Or you can enter `*ALL` for all versions.
- **Product Code** and **Reporting Code**. If you entered a specific application, form, or version, these fields automatically change to *ALL (all product codes or all reporting codes) and you cannot modify them. If you entered *ALL for the application, form, and version, you can enter a specific product or reporting code to which you want to apply security. You can enter `*ALL` for all product codes.
- **Access Level**. Click the drop-down menu to select one of the following action security levels:
  - **Create**
  - **Create and Publish**
  - **Create, Publish, Modify**
  - **Disable Create, Publish, and Modify**

    Use this last option to expedite the creation of UDO action security records. For example, if you want to authorize all but two members of a role to "create, publish, and modify" UDOs, you create one record for the role authorizing "Create, Publish, Modify;" and then create two records using this "Disable Create, Publish, and Modify" option to prevent the two users from creating UDOs.

5. As an alternative to using the Access Level drop-down menu, you can click the icons in the Create, Publish, or Modify columns to activate or deactivate the action security level. A green circle indicates the action is active, a red square indicates the action is inactive.

   When using the icons to select the security level, the security level is reflected in the Access Level column in the grid.
6. Click the **Save** button to save the record.

To modify UDO action security:

1. In Security Workbench, select the **Form** menu, **User Defined Object**, **Action**.
2. On Work With User Defined Object Action Security, click the **Find** button to access Action security records. You can refine the search by using filter fields in the header row of the grid.
3. Click the icons in the following columns to modify the UDO action security:
   - Create
   - Publish
   - Modify

     The Access Level field in the row will change to reflect the modified action security.

     Also, a warning appears reminding you to clear the security cache for the changes to take effect.

To delete UDO action security:

1. In Security Workbench, select the **Form** menu, **User Defined Object**, **Action**.
2. On Work With User Defined Object Action Security, click the **Find** button to access Action security records. You can refine the search using the filter fields in the header row of the grid.
3. Click the check box next to the records you want to delete and then click the **Delete** button.

> **Note:** To disable UDO action security, you do not have to delete the UDO action security record. Instead, you can disable the security record by making it inactive. This enables you to save the record in case you choose to make it active again at another time.

Managing UDO View Security

This section contains the following topics:

- *Understanding UDO View Security*
- *Managing UDO View Security from Security Workbench*
- *Managing UDO View Security from P98220U*
- *Setting Up Base Form Security (Release 9.2.4)*

Understanding UDO View Security

Set up UDO view security to authorize access to shared UDOs. Shared UDOs are secure by default; other users cannot access them unless authorized to do so through UDO view security.

> **Note:** To share a UDO, the creator of the UDO has to click the "Request to Publish" button, which sends it through an approval process. After the UDO is approved by an approver in the User Defined Object Management (P98220U) application, it is considered a "shared UDO." **See Also**: *JD Edwards EnterpriseOne Tools Using and Approving User Defined Objects Guide* for information on how to approve UDOs.

You can set up UDO view security for:

- Individual shared UDOs.
- All shared UDOs of a particular UDO type. Instead of specifying the name of a particular shared UDO, you can enter `*ALL` for the "User Defined Object Name" to gives users access to all shared UDOs of a particular UDO type. For example, for grid formats, if you enter *ALL instead of the name of a particular shared grid format, users will be able to access all grid formats that are shared.

  > **Note:** You cannot use *ALL for Classic EnterpriseOne Pages and Composed Pages. This restriction prevents users from being able to access all Classic and Composed Pages from the EnterpriseOne Welcome screen. (Release 9.2.0.2)

  > **Note:** You must first request to share the Classic EnterpriseOne Page and receive View permissions from your system administrator before your page is available in run time.

- (Release 9.2.4) *BASE value for the personal forms UDO type.

System administrators can use the *BASE value to restrict access to an EnterpriseOne form so that users can access only the personalized forms available to them and not the base form.

> **Note:** When setting up base form security using the *BASE value, system administrators cannot use a combination of *ALL in the Application Name column and *BASE in the User Defined Object Name column. This restriction prevents system administrators from restricting access to all applications.

You set up UDO view security records for a user, role, or *PUBLIC (all users). In addition, you can define a particular application, form, application version, product code, or reporting code to which to apply the security. Or you can use *ALL (all objects) to apply view security to all applications, forms, application version to which the user has access.

EnterpriseOne provides two versions of the "Work With User Defined Object View Security" form:

- **W00950UOG**. Access this form through Security Workbench. Use this form to set up view security for individual UDOs or all shared UDOs of a particular UDO type. Setting up view security for all shared UDOs of a particular UDO type can only be performed using this form. Starting with EnterpriseOne Tools Release 9.2.3, you can access W00950UOG from the User Defined Object Management (P98220U) application.
- **W00950UOK**. Access this form outside of Security Workbench through the User Defined Object Management (P98220U)application, the application for reviewing, approving, or rejecting UDOs submitted for sharing. This enables you to allow the same user approving UDOs to set up view security for the objects. Oracle recommends using this application to set up UDO view security for individual shared UDOs.

Updates to UDO view security in either form are reflected in both forms.

Managing UDO View Security from Security Workbench

Access the W00950UOG form in Security Workbench to set up view security for individual UDOs or all shared UDOs of a particular UDO type. Setting up view security for all shared UDOs of a particular UDO type can only be performed using this form.

> **Note:** If you add, modify, or delete view security, users must clear the cache in the browser for the changes to take effect.

To set up UDO view security for all shared UDOs of a particular UDO type:

1. On Work With User/Role Security in the Security Workbench (P00950), select the **Form** menu, **User Defined Object**, **View**.

   Alternatively, on Work with User Defined Objects (P98220U), select the Form menu, and then select View Security. (Release 9.2.3)
2. On Work With User Defined Object View Security (W00950UOG), click the **Add** button.
3. On User Defined Object View Security, click the search button in the Object Type field and select a UDO type. For a complete list of User Defined Objects, see the JD Edwards EnterpriseOne Tools Using and Approving User Defined Objects Guide.

   > **Note:** For **IMAGE** UDOs, view security is set up by default. Users can access all the shared images. (Release 9.2.0.2)

4. In the first row in the grid, complete the following columns:
   - **User/Role**. Enter a user, role, or enter `*PUBLIC` for all users.
   - **Application Name**. If you want access to shared UDOs limited to a particular application, enter the application ID. Or you can enter `*ALL` if you want the shared UDO to be available in all applications.
   - **Form Name**. If you want access to shared UDOs limited to a particular form, enter the form ID. Enter `*ALL` for all forms.
   - **Version**. If you want access to shared UDOs limited to a particular application version, enter the version ID. Or you can enter `*ALL` for all versions.
   - **User Defined Object Name**. Enter `*ALL` to allow access to any shared UDO of the selected UDO type (Object Type).
   - **Product Code and Reporting Code**. If you entered a specific application, form, or version, these fields automatically change to *ALL (all product codes or all reporting codes) and you cannot modify them. If you entered *ALL for the application, form, and version, you can enter a specific product or reporting code to which you want to apply security. Enter `*ALL` for all product codes.
5. Click the **Save** button.

To set up view security for individual shared UDOs:

1. In Security Workbench (P00950), select the **Form** menu, **User Defined Object**, **View**.

   Alternatively, on Work with User Defined Objects (P98220U), select the Form menu, and then select View Security. (Release 9.2.3)
2. On Work With User Defined Object View Security, click the **Add** button.
3. On User Defined Object View Security, click the search button in the Object Type field and select a UDO type. For a complete list of User Defined Objects, see the JD Edwards EnterpriseOne Tools Using and Approving User Defined Objects Guide.

   > **Note:** For **IMAGE** UDOs, view security is setup by default. Users can access all the shared images. (Release 9.2.0.2)

4. In the first row in the grid, complete the following columns:

   > **Tip:** Use the Work with User Defined Objects application (P98220U) to generate a list of shared UDOs. In the grid, you can export the shared UDO records to a spreadsheet so you can easily see detailed information about the shared UDOs.

   - **User/Role**. Enter a user, role, or enter *PUBLIC for all users.
   - **Application Name**. If you want access to a shared UDO limited to a particular application, enter the application ID. You can enter `*ALL` if you want the shared UDO to be available in all applications.
   - **Form Name**. If you want access to a shared UDO limited to a particular form, enter the form ID. Or you can enter `*ALL` for all forms.
   - **Version**. If you want access to a shared UDO limited to a particular application version, enter the version ID. You can enter `*ALL` for all versions.
   - **User Defined Object Name**. Enter the name of the shared UDO.
   - **Product Code and Reporting Code**. If you entered a specific application, form, or version, these fields automatically change to *ALL (all product codes or all reporting codes) and you cannot modify them. If you entered *ALL for the application, form, and version, you can enter a specific product or reporting code to which you want to apply security. Enter `*ALL` for all product codes.
5. Click the **Save** button.

To modify UDO View security:

1. In Security Workbench (P00950), select the **Form** menu, **User Defined Object**, **View**.

   Alternatively, on Work with User Defined Objects (P98220U), select the Form menu, and then select View Security. (Release 9.2.3)
2. On Work With User Defined Object View Security, click the **Find** button to load the UDO view security records in the grid.

   You can use the filter fields in the header row of the grid to refine your search.
3. In the View column, click the icon in the row to change the status to Active or Inactive.

   A green circle indicates the security record is active. A red square indicates the security record is inactive. You can hover over the icon to display the status in text.

To delete UDO View security:

1. In Security Workbench (P00950), select the **Form** menu, **User Defined Object**, **View**.

   Alternatively, on Work with User Defined Objects (P98220U), select the Form menu, and then select View Security. (Release 9.2.3)
2. On Work With User Defined Object View Security, click the **Find** button to load the UDO view security records in the grid.
3. Click the check box next to the records that you want to delete, and then click the **Delete** button.

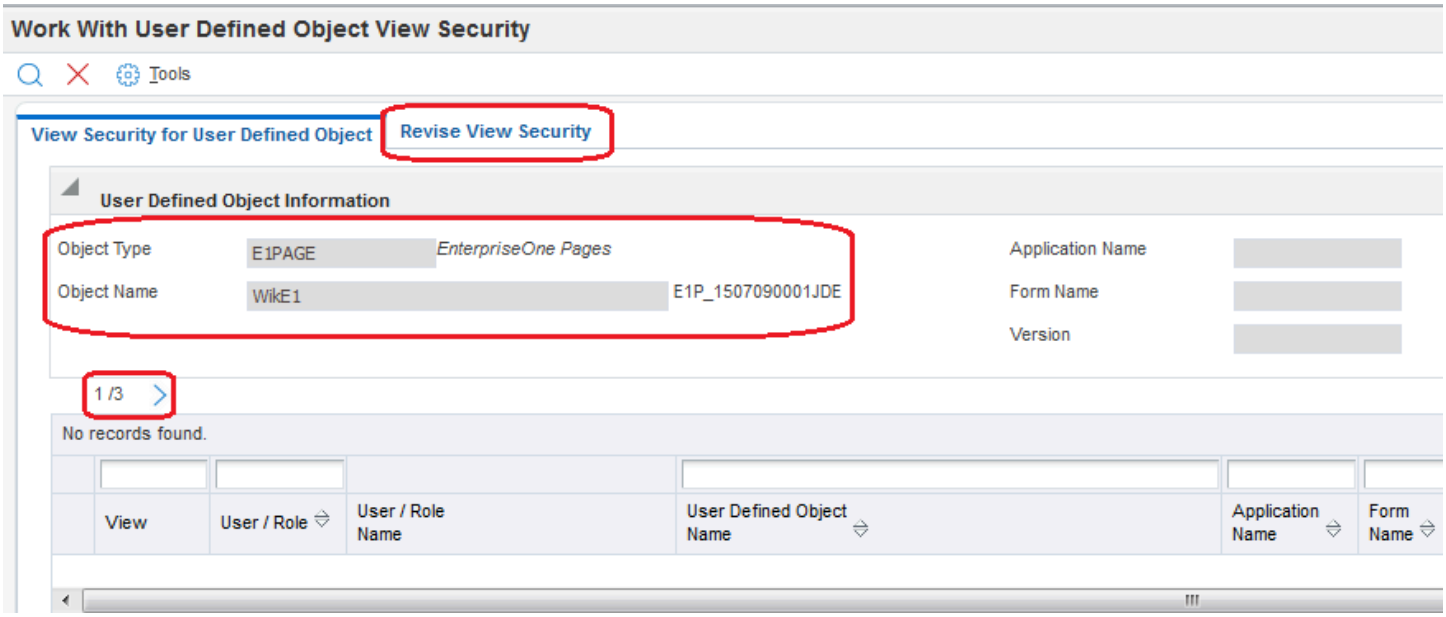
> **Note:** To disable UDO view security, you do not have to delete the security record. Instead, you can disable the security record by making it inactive. This enables you to save the record in case you choose to make it active again in the future.

Managing UDO View Security from P98220U

In P98220U, you can access a version of the Work With User Defined Object View Security form (W00950UOK) to set up UDO view security. This enables the same user approving UDOs to easily set up view security for the UDOs.

> **Note:** You must set up permissions to allow access to W00950UOK from P98220U. See *Enable Access to UDO Security and Administration Applications* for more information.

In P98220U, you can select one or more UDOs that have been approved for sharing (UDO Status = Shared) and then access W00950UOK to set up view security for the selected records. If multiple shared UDOs were selected in P98220U, the first record is displayed in the header area on the View Security for User Defined Object tab. The following illustration shows the first of three shared UDO records:



On this form, you can:

- Revise any existing view security records for the selected UDO. If view security was already applied to the UDO, a list of the view security records for the UDO would appear in the grid. In the preceding example, there are no view security records, so you would have to click the **Revise View Security** tab to set up view security.
- Select the **Revise View Security** tab to add view security records for the selected UDO.
- If multiple UDOs were selected in P98220U, you can click the right directional arrow to access and set up view security for the other UDOs.

Note: If you add, modify, or delete view security, users must clear the cache in the browser for the changes to take effect.

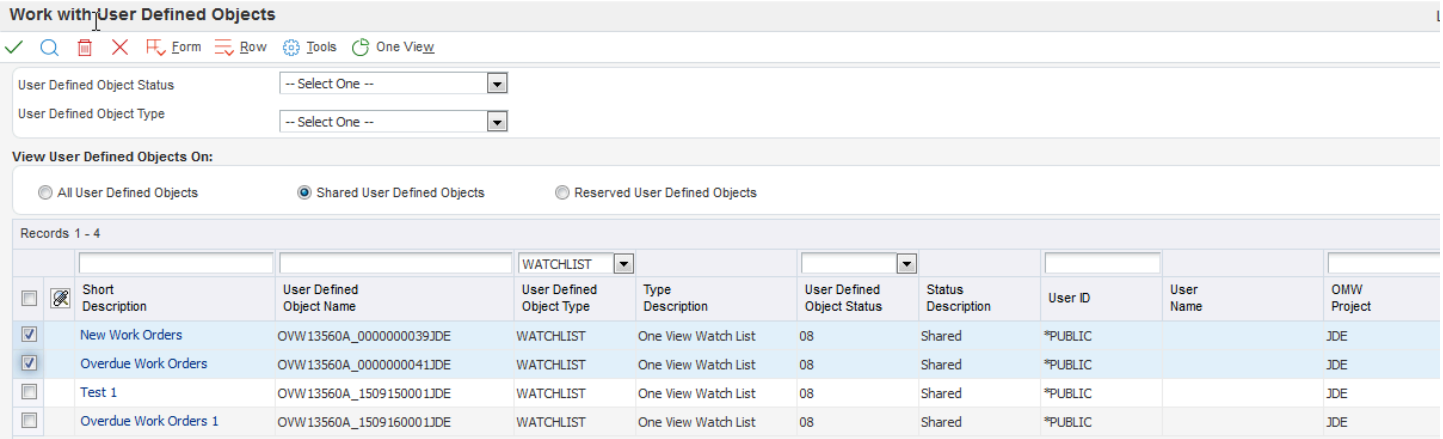
Navigation to P98220U: On the EnterpriseOne Welcome Page, select the Navigator menu, EnterpriseOne Menus, EnterpriseOne Life Cycle Tools, System Administration Tools, User Defined Object Tools, User Defined Object Administration.

To create UDO view security records in W00950UOK:

1. On Work with User Defined Objects, in the "View User Defined Objects On" area, select the **Shared User Defined Objects** option to load all shared UDOs in the grid.

   Shared UDOs have been approved for sharing and have a status of "Shared" in the Status Description column.

2. You can use the User Defined Object Status and User Defined Object Type fields in the header area or the filter fields in the header row in the grid to refine your search.



3. In the first column in the grid, click the check box of the shared UDO for which you want to set up view security.

   You can select multiple rows to set up view security for multiple UDOs.
4. Select the **Row** menu, **Advanced**, **Security**.

   EnterpriseOne displays the shared UDOs in the Work With User Defined Object View Security form. If you selected multiple records, the first record is displayed in the header area. You can click the right arrow to access each shared UDO record for which you want to set up view security.
5. On Work With User Defined Object View Security (W00950UOG), click the **Revise View Security** tab.
6. In the first row in the grid, complete the following columns:
   - **User/Role**. Enter a user, role, or enter `*PUBLIC` for all users.
   - **Application Name**. If you want access to a shared UDO limited to a particular application, enter the application ID. Or you can enter `*ALL` if you want the shared UDO to be available in all applications.
   - **Form Name**. If you want access to a shared UDO limited to a particular form, enter the form ID. You can enter `*ALL` for all forms.
   - **Version**. If you want access to a shared UDO limited to a particular application version, enter the version ID. You can enter `*ALL` for all versions.
   - **Product Code** and **Reporting Code**. If you entered a specific application, form, or version, these fields automatically change to *ALL (all product codes or all reporting codes) and you cannot modify them. If you entered *ALL for the application, form, and version, you can enter a specific product or reporting code to which you want to apply security. Enter `*ALL` for all product codes.
7. In the View column, click the icon to activate the security record.

   A green circle indicates that the security record is active. A red square indicates that the security record is inactive. You can hover over the icon to display the status in text.

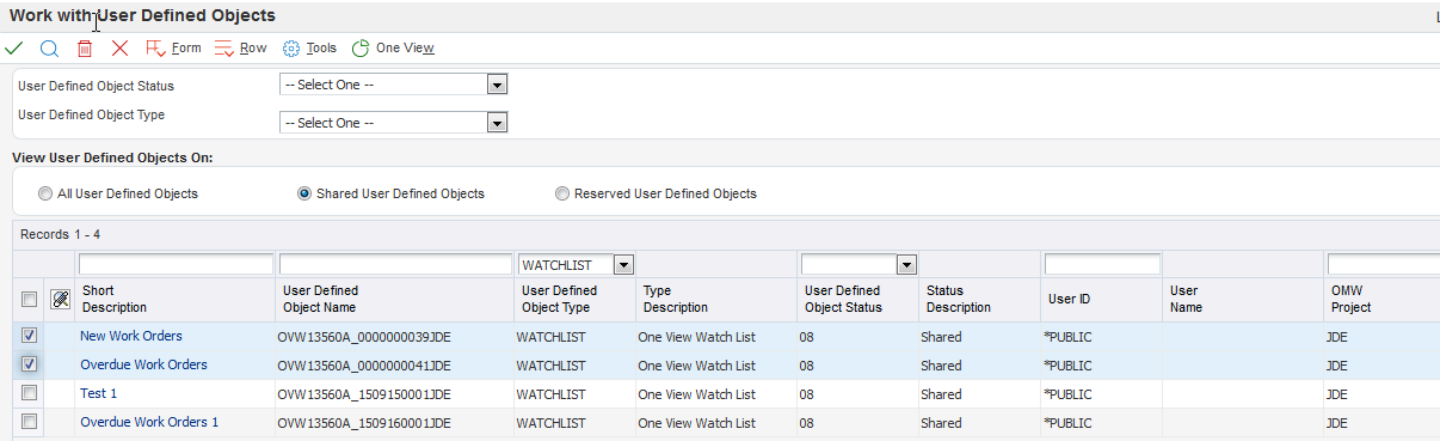
By default, view security is inactive unless you make it active. You must make sure that view security is active for users to use the shared UDO.

8. Click the **Save** button.
9. If you make a mistake and save a record that you do not want to keep, before exiting the form, select the record in the grid and click the **Delete** button.

To modify UDO view security records in W00950UOK:

1. On Work with User Defined Objects (P98220U), in the "View User Defined Objects On" area, select the "Shared User Defined Objects" option to load all shared UDOs in the grid. You can use the fields in the header area or the filter fields in the header row in the grid to refine your search.

   Shared UDOs are approved for sharing and have a status of "Shared" in the Status Description column.



2. In the first column in the grid, click the check box of the shared UDO for which you want to modify UDO view security. You can select more than one record if you want to revise UDO view security for multiple records.
3. Select the **Row** menu, **Advanced**, **Security**.

   EnterpriseOne displays the shared UDOs in the Work With User Defined Object View Security form. If you selected multiple records, the first record is displayed in the header area. You can click the right arrow to access the other selected shared UDOs.
4. On the View Security for User Defined Object tab, click the icon to activate or deactivate any of the view security records in the grid.

   The record is automatically updated in Security Workbench after changing the status.

To delete UDO view security records in W00950UOK:

1. On Work with User Defined Objects, in the "View User Defined Objects On" area, select the **Shared User Defined Objects** option to load all shared UDOs in the grid. You can use the fields in the header area or the filter fields in the header row in the grid to refine your search.
2. In the first column in the grid, click the check box of the shared UDO for which you want to delete view security. You can select more than one record if you want to delete the view security for multiple shared UDOs.
3. Select the **Row** menu, **Advanced**, **Security**.

   EnterpriseOne displays the shared UDOs in the Work With User Defined Object View Security form. If you selected multiple records, the first record is displayed in the header area. You can click the right arrow to access the other selected shared UDOs.
4. Select the **Revise View Security** tab, select a record and then click the **Delete** button.

   > **Note:** To disable UDO view security, you do not have to delete the security record. Instead, you can disable the security record by making it inactive. This enables you to save the record in case you choose to make it active again in the future.

To manage UDO view security records by a user or a role from P98220U (Release 9.2.3)

You can access the Work With User Defined Object View Security form (W00950UOG) from the Work with User Defined Objects application (P98220U). This form gives you the option of providing the same user who is responsible for reviewing and approving shared UDOs in P98220U, the ability to set up/revise view security for shared UDOs. In addition, you can use this form to view the records to which a particular user/role has access to. All view security records created in this application are reflected in the view security form in Security Workbench.

1. In Work with User Defined Objects application (P98220U), select the Form menu, and then select View Security.
2. On Work With User Defined Object View Security, click the Find button to load the UDO view security records in the grid.

   You can use the filter fields in the header row of the grid to refine your search.

To access Work With User Defined Object View Security (W00950UOG) from P98220U:

On the Work With User Defined Object View Security (W00950UOG) form, you can:

- Set up view security for individual UDOs or all shared UDOs of a particular UDO type.
- Revise any existing view security record for a selected UDO.
- Delete the view security for a shared UDO.
- Copy the security information for another user or role. When you copy security, you can either overwrite the current security for the user or role, or you can add the new security information to the existing security information. See, *Copying All Security Records for a User or a Role*
- Copy selected security records for a user or role. You can select and copy one security record at a time or all the security records for a user or role. See, *Copying a Single Security Record for a User or a Role*

Setting Up Base Form Security (Release 9.2.4)

You can use UDO view security settings to restrict access to the base forms. A base form is an EnterpriseOne form that is designed by using the Form Design Aid (FDA) and that has not been personalized. Personalized forms are the forms

that have been personalized by using the Personal Form UDO. Configuring base form security ensures that users will only be able to access the personalized forms and not the base form.

JD Edwards EnterpriseOne provides a special UDO value, *BASE, that system administrators can use to configure base form security. When setting up base form security for an EnterpriseOne application, the system administrator must enter the *BASE value manually in the User Defined Object Name field on the User Defined Object View Security form.

If base form security is configured, the system determines the form that will be displayed when a user accesses the application based on the following order of precedence:

1. If a default personal form exists for the user, the system displays the default personal form.
2. If a default personal form does not exist for the user, the system displays the shared default form.
3. If a shared default form does not exist for the user, the system displays the last active form.
4. If the last active form does not exist for the user, the system displays the first personal form in the Personalization drop-down menu.

If base form security is configured and a personal form does not exist for the user, the system displays the base form but hides the Personal Form icon. This means that the user cannot personalize the form by using the Personal Form UDO.

To configure base form security:

1. On Work With User/Role Security in the Security Workbench (P00950), from the **Form** menu, select **User Defined Object** and then select **View**.

   Alternatively, on Work with User Defined Objects (P98220U), select the **Form** menu, and then select **View Security**.
2. On Work With User Defined Object View Security (W00950UOG), click **Add**.
3. On User Defined Object View Security, click the search button in the Object Type field and select PERSFORM (personal forms) as the UDO type. For a complete list of user defined objects, see the *JD Edwards EnterpriseOne Tools Using and Approving User Defined Objects Guide*.
4. In the first row in the grid, ensure that the View column displays a red square and then complete the following columns:
   - **User/Role**. Enter a user, role, or enter `*PUBLIC` for all users.
   - **Application Name**. Enter the application ID of the application which you want to secure.

     > **Note:** If you enter *ALL in this field and *BASE in the User Defined Object Name field, the system displays an error message.

   - **Form Name**. Enter the form ID of the form for which you want to configure base form security. Enter `*ALL` for all forms.
   - **Version**. Enter the version ID of the If you want to limit the base form security to a particular application version, enter the version ID. Or you can enter `*ALL` for all versions.
   - **User Defined Object Name**. Enter `*BASE`.

     > **Note:** *BASE is a special value and is not available as a UDC value. Therefore, you must manually enter this value in the User Defined Object Name field.

   - **Product Code and Reporting Code**. If you entered a specific application, form, or version, these fields automatically change to *ALL (all product codes or all reporting codes) and you cannot modify them.
   - **Web Object Category**. Enter PERSFORM.
5. Click **OK**.

Managing Content Security for Composite Application Framework

This section contains the following topics:

Understanding Content Security

A Composite Application Framework layout can include the following types of content:

- Embedded EnterpriseOne forms
- Generic URLs (contents from external web sites)
- Oracle Business Intelligence Enterprise Edition reports (requires additional license)

In addition to setting up action and view security for Composite Application Framework layouts, you must set up content security to authorize users to work with or view the content types in Composite Application Framework layouts. Content security records are created by content type for a user, role, or *PUBLIC by content type. Without content security, users who are authorized to view or work with a Composite Application Framework layout will not be able to view or work with its contents.

> **Note:** If you add, modify, or delete content security, users must clear the cache in their browser for the changes to take effect.

Required Security for Working with Content in Shared Composite Application Framework Layouts

The following security must be in place for users to **work with** content in shared Composite Application Framework layouts:

- Composite Application Framework feature enablement, which activates the Composite Application Framework feature globally in EnterpriseOne.
- UDO action security that allows users to create, share, or modify Composite Application Framework layouts.
- Content security that allows users to work with the following types of content in a Composite Application Framework layout: embedded EnterpriseOne forms, content from external web sites, and OBIEE content.

Required Security for Viewing Content in Shared Composite Application Framework Layouts

The following security must be in place for users to **view** content in shared Composite Application Framework layouts:

- Composite Application Framework feature enablement, which activates the Composite Application Framework feature globally in EnterpriseOne.
- UDO view security that allows access to the Composite Application Framework layout in the application. This enables users who have access to the application through EnterpriseOne application security, to access a Composite Application Framework layout associated with the application.
- Content security that allows access to the following types of content that can be included in a Composite Application Framework layout: embedded EnterpriseOne forms, content from external web sites, and OBIEE content.

Additional Setup Required for OBIEE Content in Composite Application Framework

To display OBIEE content in Composite Application Framework, you must set up an integration between EnterpriseOne and OBIEE. See the *"Configuring a Business Intelligence Connection" in the JD Edwards EnterpriseOne Tools Composite Application Framework (CafeOne) User's Guide* for more information.

Navigation to Security Workbench: On the EnterpriseOne Welcome page, select the Navigator menu, EnterpriseOne Menus, EnterpriseOne Life Cycle Tools, System Administration Tools, Security Maintenance, Security Workbench.

To set up Composite Application Framework content security:

1. In Security Workbench, select the **Form** menu, **User Defined Object**, **Content**.
2. On Work With Content, click the **Add** button.
3. On Revise Content, select **CAFE1** from the Feature drop-down menu.

   EnterpriseOne populates the grid with the three content types you can authorize access to in Composite Application Framework: Embedded E1 Form, Generic URL, and OBIEE – CafeOne Layout.
4. In the User/Role field, enter a user, role, or `*PUBLIC`.
5. In the grid, click the icon in the Access column authorize access to a content type.

   A green circle indicates that the security record is active. A red square indicates that the security record is inactive. You can hover over the icon to display the status in text.
6. Click **Save**.

To modify Composite Application Framework content security:

1. In Security Workbench, select the **Form** menu, **User Defined Object**, **Content**.
2. On Work With Content, click **Find** to access the current content security records.

   You can use the filter fields in the header row in the grid to refine your search by User/Role or Content Link (content type).
3. In the grid, click the icon in the Access column activate or deactivate access to a content type.

A green circle indicates that the security record is active. A red square indicates that the security record is inactive. You can hover over the icon to display the status in text.

To delete Composite Application Framework content security:

1. In Security Workbench, select the **Form** menu, **User Defined Object**, and then select **Content**.
2. On Work With Content, click **Find** to access the current content security records.

   You can use the filter fields in the header row in the grid to refine your search by User/Role or Content Link (content type).
3. Click the check box next to the records you want to delete and then click the **Delete** button.

> **Note:** To disable content security, you do not have to delete the security record. Instead, you can disable the security record by making it inactive. This enables you to save the record in case you choose to make it active again in the future.

Managing Content Security for Composite Page (Release 9.2.0.2)

This section contains the following topics:

- *Understanding Content Security*
- *Required Security for Working with Content in Shared Composed Pages*
- *Required Security for Viewing Content in Shared Composed Pages*
- *Additional Setup Required for OBIEE Content in Composed Page*

Understanding Content Security

A Composed Page can include the following types of content:

- Designer Pane
- One View Reports
- Embedded EnterpriseOne forms
- Classic EnterpriseOne pages
- Generic URLs (content from external web sites)
- ADF applications
- Oracle Business Intelligence Enterprise Edition reports (requires additional license)
- Watchlist Pane (Release 9.2.0.3)
- Springboard Pane (Release 9.2.1)

In addition to setting up action and view security for Composite Page, you must set up content security to authorize users to work with or view the content types in Composed Page. Content security records are created by content type for a user, role, or *PUBLIC by content type. Without content security, users who are authorized to view or work with a Composed Page will not be able to view or work with its contents.

Note: If you add, modify, or delete content security, users must clear the cache in their browser for the changes to take effect.

Required Security for Working with Content in Shared Composed Pages

The following security must be in place for users to **work with** content in shared Composed Pages:

- Composite Page feature enablement, which activates the Composite Page feature globally in EnterpriseOne.
- UDO action security that allows users to create, share, or modify Composed Pages.
- Content security that allows users to work with the following types of content in a Composed Page: embedded EnterpriseOne applications, content from external web sites, One View Reports, ADF applications, Classic EnterpriseOne pages, and OBIEE content.

Required Security for Viewing Content in Shared Composed Pages

The following security must be in place for users to **view** content in shared Composed Pages:

- Composite Page feature enablement, which activates the Composite Page feature globally in EnterpriseOne.
- UDO view security that allows users to view Composed Pages.

  Note: You cannot use *ALL for the "User Defined Object Name". This restriction prevents users from being able to access all Composed Pages from the EnterpriseOne Welcome screen.

- Content security that allows access to the following types of content that can be included in a Composed Page: embedded EnterpriseOne forms, content from external web sites, and One View report, ADF application, Classic EnterpriseOne page, and OBIEE content.

Additional Setup Required for OBIEE Content in Composed Page

To display OBIEE content in a Composed Page, you must set up an integration between EnterpriseOne and OBIEE.

Refer to *"Oracle BI Publisher and JD Edwards EnterpriseOne Security" in the JD Edwards EnterpriseOne Tools BI Publisher for JD Edwards EnterpriseOne Guide* for instructions on how to configure Oracle BI Publisher with EnterpriseOne.

Navigation to Security Workbench: On the EnterpriseOne Welcome page, select the Navigator menu, EnterpriseOne Menus, EnterpriseOne Life Cycle Tools, System Administration Tools, Security Maintenance, and Security Workbench.

To set up Composite Page content security:

1. In Security Workbench, select the **Form** menu, **User Defined Object**, **Content**.
2. On Work With Content, click the **Add** button.
3. On Revise Content, select **COMPOSITE** from the Feature drop-down menu.

EnterpriseOne populates the grid with the following content types you can authorize access to in Composite Page: ADF application, Embedded E1 Form, EnterpriseOne Pages, Generic URL, OBIEE - CafeOne Layout, and One View Report.

4. In the User/Role field, enter a user, role, or `*PUBLIC`.
5. In the grid, click the icon in the Access column to authorize access to a content type.

   A green circle indicates that the security record is active. A red square indicates that the security record is inactive. You can hover over the icon to display the status in text.
6. Click **Save**.

To modify Composite Page content security:

1. In Security Workbench, select the **Form** menu, **User Defined Object**, **Content**.
2. On Work With Content, click **Find** to access the current content security records.

   You can use the filter fields in the header row in the grid to refine your search by User/Role or Content Link (content type).
3. In the grid, click the icon in the Access column to activate or deactivate access to a content type.

   A green circle indicates that the security record is active. A red square indicates that the security record is inactive. You can hover over the icon to display the status in text.

To delete Composite Page content security:

1. In Security Workbench, select the **Form** menu, **User Defined Object**, and then select **Content**.
2. On Work With Content, click **Find** to access the current content security records.

   You can use the filter fields in the header row in the grid to refine your search by User/Role or Content Link (content type).
3. Click the check box next to the records you want to delete and then click the **Delete** button.

> **Note:** To disable content security, you do not have to delete the security record. Instead, you can disable the security record by making it inactive. This enables you to save the record in case you choose to make it active again in the future.

> **Note:** *Click here to view a recording of Managing Content Security for User Defined Objects (UDO)*.

27 Setting Up JD Edwards Solution Explorer Security

Understanding JD Edwards Solution Explorer Security

Use the Security Workbench application (P00950) to set up security for these JD Edwards Solution Explorer features:

- Menu Design
- Menu Filtering
- Favorites
- Fast Path
- Documentation
- OMW Logging

This table describes the three general security settings for JD Edwards Solution Explorer features:

Security Setting	Description
Secured	Restricts the user from accessing the feature.
View	Allows read-only access to the feature but no modification capability.
Change	Gives the user full access to the feature with no restrictions on changing, adding, or deleting data.

In JD Edwards Solution Explorer, you can check the permissions for each feature for any user in the system. You view the settings by signing onto JD Edwards EnterpriseOne as the user whose settings you want to view, and then clicking the security button in the status bar of the JD Edwards Solution Explorer, which launches the Solution Explorer Security form. You cannot change the security settings from this form.

Note: You can also view existing Solution Explorer security records in P00950.

Users who are logged into the Microsoft Windows client can quickly identify their Solution Explorer security by double-clicking on the padlock on the status bar at the bottom of the window.

This table shows the features and provides a description of the settings for Solution Explorer Security:

Feature	Setting Description
Menu Design	Typically, administrators use the Menu Design feature to set up menus, tasks, task views, and task view roles. You use Solution Explorer to provide or limit access to the Menu Design feature for a specific user or role by selecting one of these security options: Secured - The feature is not available when the user or role signs on to the system.

Feature	Setting Description
	View - The user or role can see and use menus, tasks, task views, and task roles that you have set up. Change - The user or role can create and modify menus, tasks, task views, and task roles. The Menu Design button appears on the Microsoft Windows client when this feature is set to Change. Typically, you select the Change setting for an administrator. See "Using the Design Menu Mode" in the *JD Edwards EnterpriseOne Tools Solution Explorer Guide* .
Menu Filtering	Typically, administrators use the Menu Filtering feature to selectively enable or disable tasks by role in a task view. You use Solution Explorer to provide or limit access to the Menu Filtering feature for a specific user or role by selecting one of these security options: Secured - The Menu Filtering button is not available when the user or role signs on to the system. View - The user or role can see Menu Filtering information. Change - The user or role can hide or show tasks or task views and save changes to roles. Typically, you select the Change setting for an administrator. See "Using the Menu Filtering Mode" in the *JD Edwards EnterpriseOne Tools Solution Explorer Guide* .
Favorites	This feature enables users to save links to their tasks and access tasks directly from their Favorites task view. You use Solution Explorer to provide or limit access to the Favorites feature for a specific user or role by selecting one of these security options:Secured-The Favorites task view is not available when the user or role signs on to the system.View-Users or roles can see the Favorites task view and access tasks (assuming they have security rights for the application, form, version, and so on) from the Favorites task view; however, users or roles cannot add or remove tasks from the Favorites task view. Change-Users or roles can add and remove tasks from the Favorites task view.Typically, you select the Change option in Solution Explorer so that your users can create and change their Favorites task view. See "Understanding EnterpriseOne Navigation" in the *JD Edwards EnterpriseOne Tools Foundation Guide* .
Fast Path	The Fast Path feature is used by your users to navigate to menus, folders, applications, and reports directly. Your users enter commands in the Fast Path to move quickly among menus and applications. You use Solution Explorer to provide or limit access to the Fast Path feature for a specific user or role by selecting one of these security options: Secured - The Fast Path command line is not available when the user or role signs on to the system. View - The user or role can enter tasks, fast path codes, or applications in the Fast Path command line. Restricted View (menu navigation and mnemonics only) - The user or role can use the Fast Path command line to call menus and applications that are defined in the Fast Path UDC table. This option prevents the user or role from running tasks that call applications directly or from accessing specific objects by entering an object name. For example, users with the Restricted View option receive an error if they attempt to launch an application directly by typing in the object name (such as P01012) or if they attempt to type in a task ID for a task that launches an interactive or batch application. See "Understanding EnterpriseOne Navigation" in the *JD Edwards EnterpriseOne Tools Foundation Guide.*
Documentation	The Documentation feature enables users to access online Documentation for a task. You use Solution Explorer to provide or limit access to the Documentation feature by selecting one of these options:Secured - The documentation feature is not available to the user or role. View - The user or role can view available online documentation for a task. Typically, you select this setting for users or roles.Edit - The user or role can edit the online task documentation. Task documentation can be edited only from a Windows client. Users or roles using a Web client cannot edit task documentation. Users

Feature	Setting Description
	access documentation by clicking the arrow to the right of the task, and then selecting *Documentation*. A task may have multiple types of documentation, which appears as separate selections.
OMW Logging	You use Solution Explorer to enable (on option) or disable (off option) the OMW Logging feature for a specified user or role. When enabled, the OMW Logging feature captures information when a user uses Object Management Workbench (OMW) to transfer Solution Explorer task information between environments.

Note: When you use Solution Explorer security options for a user or role, be sure to select the appropriate option for each feature on the form.

Fast Path Security Settings

Besides preventing or allowing access to Fast Path, you can also set up Fast Path access in a restricted view. The restricted view prevents web client users from entering an application ID in the Fast Path to launch an application. Instead, users can enter menu IDs to access menus in the EnterpriseOne Menus. The menu ID must be associated to a menu in the Task Master table (F9000).

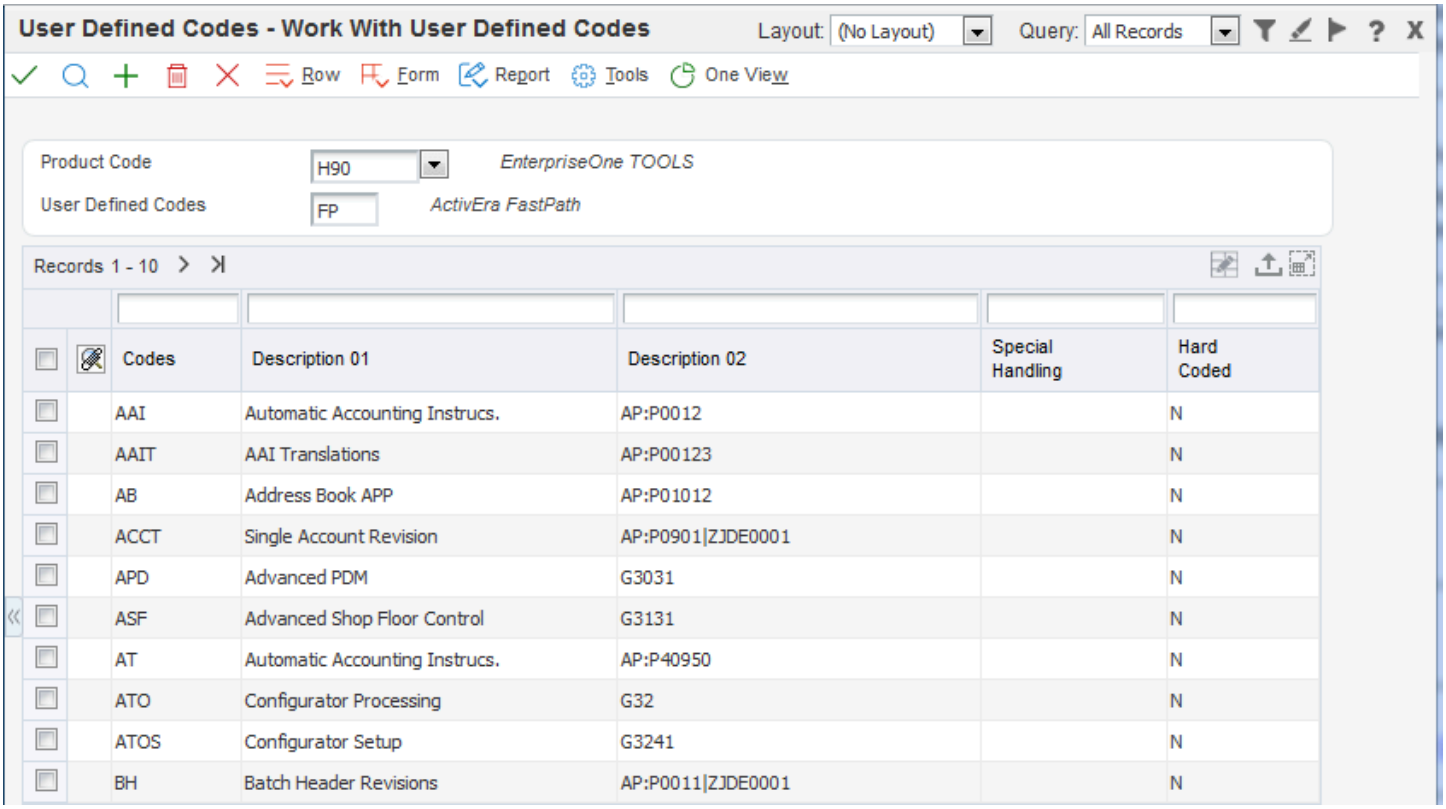
The restricted view also allows users to enter a mnemonic code, defined in the User Defined Code Values table (F0005), to launch an application or access a menu.

You can add UDCs for mnemonic codes using the User Defined Codes application (P0004A). Use these parameters when adding UDCs for mnemonic codes in P0004A:

- Product Code: H90 (EnterpriseOne Tools)
- UDC Type: FP

Note: After you add UDCs for mnemonic codes, you must clear the cache in order for the UDCs to take affect in the system. See *Cached Security Information*.

The following example shows some of the mnemonic codes already defined in JD Edwards EnterpriseOne.



To set up UDCs for mnemonic codes, refer to the instructions on how to customize and add UDCs.

See *"Working with User Defined Codes" in the JD Edwards EnterpriseOne Tools Runtime Administration Guide.*

Solution Explorer Security Presets

Security Workbench (P00950) contains security presets that determine default security settings for different types of users. These security presets correspond to novice (Preset One), intermediate (Preset Two), and expert (Preset Three) users. If you click one of these preset buttons, Solution Explorer changes the Security Revisions default settings for each feature.

Novice users require the most restrictive security settings; expert users require the least restrictive settings. Although you can fine-tune these default settings for a particular individual, using the default settings can free you from the task of manually choosing security setting options for each individual in the system because you can apply the settings to groups as well as to individual users.

Prerequisite

Fast Path Restricted View security is a JD Edwards EnterpriseOne Tools feature that is applicable to the JD Edwards EnterpriseOne Applications 8.12 and subsequent releases.

Configuring JD Edwards Solution Explorer Security

Access the Work With User/Role Security form. In Solution Explorer, enter **P00950** in the Fast Path.

1. Select the Form menu, Setup Security, Solution Explorer.
2. On the Work with Solution Explorer Security Revisions form, enter a user ID or role in the User/Role field.
3. Select the security options for Menu Design, Menu Filtering, and Documentation, as appropriate:
   - Secured
   - View
   - Change
4. For Fast Path, select one of these options:
   - Secured
   - View
   - Restricted View (menu navigation and mnemonics only)
5. Select one of these options to enable or disable OMW Logging:
   - Off
   - On
6. Alternatively, you can select any of these options from the Preset drop-down menu to specify default Solution Explorer security settings:
   - Preset One
   - Preset Two
   - Preset Three

28 Setting Up Address Book Data Security

Understanding Address Book Data Security

The Address Book data security feature enables you to restrict users from viewing address book information that you have determined is private, personal data. After performing the required setup for this feature, secured users can see the fields that you specify as secured, but the fields are filled with asterisks and are disabled. You can set up data security for these fields:

- Tax ID
- Addl Ind Tax ID (additional tax ID)
- Address

  Includes Address Lines 1-7, City, State, Postal Code, Country, and County.
- Phone Number

  Includes phone number and phone prefix.
- Electronic Address

  Includes only electronic addresses with Type E.
- Day of Birth, Month of Birth, and Year of Birth.
- Gender

Note: In addition to these fields, the system enables you to designate up to eight other user-defined fields as secured. Included in the eight fields are: five string, one math numeric, one character, and one date type. To secure additional fields, you must modify the parameter list in the call to the business function B0100095. For example, if you want to designate Industry Class as a secured field, you must modify the call to the B0100095 business function to map Industry Class in the parameter list.

The Address Book data security feature provides an additional level of security by not allowing secured users to locate valid personal information using the query based example (QBE) line. For example, if a user enters numbers in the Tax ID field of the QBE line, the system does not display the matching record in the event that the user happens to enter a valid tax ID number.

Setting up Address Book data security involves these steps:

1. Selecting the Activate Personal Data Security constant in the Address Book Constants.

   Personal data security is inactive unless the Activate Personal Data Security constant is selected.
2. Setting up permission list definitions.

   Use the Address Book Data Permissions application (P01138) to create one or more permission lists that specify which fields in the Address Book are secured.
3. Setting up permission list relationships.

   Use the Permission List Relationships application (P95922) to determine the users or roles that are subject to each permission list.

After you set up Address Book data security, users cannot view information in the fields that you specify as secured. The secured fields appear as asterisks and the system disables these fields for updates. However, users can view their own secured address book information. Also secured fields are not protected when adding new address book records.

In addition to storing Address Book privacy data in the Address Book Data Permission List Definition table (F01138), the system stores privacy data in these tables:

- Address Book-Who's Who (F0111)
- Address Book-Phone Numbers (F0115)
- Address by Date (F0116)

During processing, when the system encounters a record that has privacy data, that record will not appear in reports, Universal Batch Engine (UBE) results, the Data Browser, and the Universal Table Browser (UTB).

Additional Level of Private Data Security

In addition to storing Address Book privacy data in the Address Book Data Permission List Definition table (F01138), the system stores privacy data in these tables:

- Address Book-Who's Who (F0111)
- Address Book-Phone Numbers (F0115)
- Address by Date (F0116)

When a user runs a report or an application other than the Address Book (such as a Universal Batch Engine report, the Data Browser, or the Universal Table Browser), if EnterpriseOne encounters secured private data in any of the tables in the preceding list, records or columns with secured data do not display in the results. The results displayed depend on whether the fetch is over one or multiple tables. If the fetch is over one table with a secured field, the records that contain secured private data do not appear in the output. If a fetch is over a business view with two tables, the records are displayed, but the columns with secured private data are blank.

For example, if an administrator configures private data security to prevent users of a role from viewing the Tax ID for search type E, and the Who's Who application is launched for an address book record with search type E, a user assigned to this role cannot view records for this Address Book record in the Who's Who application.

> **Note:** When Address Book data security is configured, you can either enable or disable the additional level of security that prevents secured private data from appearing in other applications and output. See *Enabling or Disabling Secured Private Data from Displaying in Other Applications and Output* for more information.

Prerequisites

Select the Activate Personal Data Security constant in the Address Book Constants.

See *"Setting Up the JD Edwards EnterpriseOne Address Book System" in the JD Edwards EnterpriseOne Applications Address Book Implementation Guide.*

Set up users and roles in the User Profiles application (P0092) for each user that you want to secure from Address Book information.

See *Setting Up User Profiles*.

Setting Up Permission List Definitions

This section provides an overview of permission list definitions and discusses how to set up permission list definitions.

Understanding Permission List Definitions

The Permission List Definition application enables you to create multiple lists that determine which Address Book fields are secure. When you create permission lists, you specify a permission list name and a search type, and then select each field that you want to secure. The system stores permission list definitions in the F01138 table.

Forms Used to Set Up Permission List Definitions

Form Name	FormID	Navigation	Usage
Work With Permission List Definitions	W01138A	Enter **P01138** in the Fast Path.	Review existing permission list definitions.
Add/Edit Permission List Definitions	W01138B	Select Add from the Work With Permission List Definitions form.	Create new permission list definitions or revise existing definitions.

Creating Permission List Definitions

Access the Add/Edit Permission List Definitions form.

After entering the Permission List Name and the Search Type, select each field that you want to secure.

Permission List Name
Enter a name for the permission list. Enter up to 15 alphanumeric characters.

Search Type
Select the search type for which the permission list applies.

Setting Up Permission List Relationships

This section provides an overview of permission list relationships and discusses how to set up permission list relationships.

Understanding Permission List Relationships

After you set up permission list definitions, use the Permission List Relationships application to assign them to previously defined user IDs and roles. You can attach a user ID or role to only one permission list. The system stores permission list relationships in the F95922 table.

Forms Used to Create Permission List Relationships

Form Name	FormID	Navigation	Usage
Work With Permission List Relationships	W95922A	Enter **P95922** in the Fast Path.	Search for a permission list.
Maintain Permission List Relationships	W95922D	Click Select on the Work With Permission List Relationships form.	Set up permission list relationships.

Creating Permission List Relationships

Access the Maintain Permission List Relationships form.

1. In the User or Role field, enter the User ID or Role that you want to attach to a permission list, and then click the find button.
2. Click the right arrow button to attach a User ID or Role to a permission list.
3. Click the left arrow button to remove a User ID or Role from a permission list.

Enabling or Disabling Secured Private Data from Displaying in Other Applications and Output

EnterpriseOne provides INI file settings to enable or disable the displaying of records with secured private data in applications and output other than the Address Book.

The settings for enabling and disabling this additional level of private data security are located in the JDBJ.INI file on the HTML Server and the JDE.INI file on the Enterprise Server. Use Server Manager to modify these settings:

INI File	Section and Setting	Values
JDBJ.INI on the HTML Server	[JDBj-RUNTIME PROPERTIES] enableDataPrivacySkipRecord=	Values are: **true**: Excludes records with secured data from all other output sources.

INI File	Section and Setting	Values
		false (or leave blank): This is the default. Allows records with secured data to appear in other output sources.
JDE.INI file on the Enterprise Server	[DB SYSTEM SETTINGS] enableDataPrivacySkipRecord	Values are: **true**: Excludes records with secured data from all other sources of output. **false** (or leave blank): This is the default. Allows records with secured data to appear in other output sources.

For more information about modifying INI file settings in Server Manager, see the *JD Edwards EnterpriseOne Tools Server Manager Guide* .

29 Setting Up Business Unit Security

Understanding Business Unit Security

JD Edwards EnterpriseOne business unit security provides the ability to filter data by business unit for UDCs and for transaction tables. For UDCs, you create subgroups of values that can be shared among various business units or may be unique to one particular business unit. This is referred to as UDC sharing. For transaction tables, business unit security enables you to limit the transaction records that a user has access to based on business unit. This is called transaction security.

UDC Sharing

With UDC sharing, JD Edwards EnterpriseOne provides the ability to control, or regulate, how organizational data among different business units is shared. UDC sharing enables you to define a subset of UDC values for a business unit. You can share multiple UDC values among multiple business units.

For example, a company's customer service department may provide support for appliances, consumer electronics, and sporting goods. Typically, a representative would choose from an extensive list of values to specify the repair code for a particular type of product. However, with UDC sharing, the company can associate a subset of the repair code UDC values, such as for appliances, to a business unit. As a result, the representatives associated with the business unit would only have to choose from a list of repair codes relevant to appliances.

> **Note:** UDC sharing can impact system performance because of the time it takes the system to determine the UDC values that are associated with each business unit.

Transaction Security

Another feature of JD Edwards EnterpriseOne business unit security is transaction security. Transaction security enables you to determine the transaction records a user can view. Transaction security ensures that users can only access and modify transaction data for the business unit to which they are associated.

> **Note:** *"Setting Up Business Units" in the JD Edwards EnterpriseOne Applications Financial Management Fundamentals Implementation Guide* .

Working with UDC Sharing

This section provides overviews of the UDC sharing setup and business unit security for UDC sharing and discusses how to:

- Set up UDC sharing.
- Set up business unit security for UDC sharing.

- Revise a UDC group.
- Delete a UDC group.

Understanding the UDC Sharing Setup

Use the UDC Sharing application (P95310) to set up UDC sharing. This wizard-like application leads you through the appropriate tasks to configure these items:

- UDC group

  A UDC group serves as a container for the UDC values that you want to share among different business units. You create the UDC group by naming it and assigning the UDC types that contain UDC values. For example, if you are sharing UDC values that represent various states and countries in geographic regions, you might name the UDC group GEO, and then assign the UDC types that contain the appropriate UDC values for the states or countries.
- Set-ID

  A set-ID enables you to further categorize the UDC values within a UDC group. For example, you can further categorize the UDC values in the GEO UDC group into subsets, such as Europe, Canada, Pacific Rim, and so forth. Each subset, or set-ID, can contain values that are specific to that region.

> **Note:** UDC sharing is available for JD Edwards EnterpriseOne Application Release 8.11 and later releases. You must use a Microsoft Windows client to set up UDC sharing. However, the actual security applied to applications that are run only on the web client.

Understanding Business Unit Security for UDC Sharing

JD Edwards EnterpriseOne provides a wizard-like application to assist you with setting up business unit security for UDC sharing. The application leads you through these tasks:

- Define a business unit type.

  A business unit type serves as a logical grouping of business units. To define it, you give it a name and then specify the table (typically the F0006 table) and the data item within the table that contains the business unit values.
- Associate a user ID or role to a business unit.

  > **Note:** You can associate users to business units when setting up UDC sharing or when setting up transaction security.
- Associate a UDC group to a business unit.

Setting Up UDC Sharing

Enter **GH9052** in the Fast Path, select Security Maintenance, select Business Unit Security, and then select Set-up UDC Sharing to access the UDC Group Revisions form.

Note: You can access this form on the Microsoft Windows client and the web client.

1. Complete these fields to name and describe the UDC group:
   - UDC Group
   - Group Description
2. In the detail area, click the search button in these fields to add UDC types to the UDC group:
   - Product Code
     Select the product code of the UDC type that you want to add.
   - User Defined Code
     Select the UDC type that contains the values for the UDC group.
     Note: A UDC type cannot be associated with more than one UDC group.
3. Click Next.
4. On Set-ID Definition Revisions, complete these fields to create set-IDs for the UDC group:
   - Set-ID
     Enter a name for the set-ID.
   - Description
5. Click Next.
   On Maintain Set-ID, in the right pane, the system displays the UDC types that you assigned to the UDC group. The left pane contains the set-IDs that you defined for the UDC group.
6. Assign UDC values to the Set-IDs.
   a. Select a set-ID in the left pane.
   b. Click a UDC type in the right pane, and then select from the list of UDC values.
   c. Click the left arrow to assign the UDC value to the chosen Set-ID.
7. After you assign UDC values to the set-IDs, click Done.

Setting Up Business Unit Security for UDC Sharing

Enter **GH9052** in the Fast Path, select Security Maintenance, Business Unit Security, and then select Set-up Business Unit Security to access the Business Unit Security Definition Revisions form.

1. Complete these fields in this order:
   - Business Unit Type
   - Business Unit Definition Table
     Enter the table object name that contains the individual business unit values (for example, F0006).
   - Business Unit Definition Data Item
     Enter the data item in the Business Unit Definition Table that contains the unique business unit name (for example, MCU).
2. Press Tab and then click Next to continue.

3. On User/Role to Business Unit Relationships, assign the users or roles in the right panel to the appropriate business units in the left panel.
   You can search for particular business unit values and users or roles by clicking the search button next to the Business Unit Value and User/Role fields, respectively.

   Note: You can click the Skip button if you choose not to perform this step at this time. You can also assign users to business units when setting up transaction security.

4. After securing users to the appropriate business units, click Next to continue.
5. On Maintain Transaction Security Tables, click the Skip button.
   This form is only used for transaction security.
6. On UDC Group/Set-ID/Business Unit Relationship, assign the set-IDs within the UDC groups to the appropriate business units in the left panel.
   You can search for particular business unit values and UDC groups by clicking the search button next to the Business Unit Value and UDC Group fields, respectively.
   Remember that you must first configure UDC sharing to be able to assign set-IDs to business units on this form.
7. Click Done.

Revising UDC Groups

Enter **GH9052** in the Fast Path, select Security Maintenance, Business Unit Security, and then select Maintain UDC Sharing to access the Work With UDC Sharing form.

You can access this form in the Microsoft Windows client and the web client.

1. Select the UDC group that you want to revise.
2. To add or delete a UDC type in a UDC group, from the Row menu, select Group Revisions.
3. To add or delete a set-ID, from the Row menu, select Set-ID Definition.

   Note: You cannot delete a set-ID that is part of a business unit and UDC group relationship.

4. To revise the UDC values that are assigned to the set-IDs, from the Row menu, select Maintain Set-ID.

Deleting a UDC Group

On the Work With UDC Sharing form, select the UDC group and then click Delete.

Note: You cannot delete a UDC group that is part of a business unit relationship.

Working with Transaction Security

This section provides an overview of how to set up transaction security and discusses how to:

- Set up transaction security.

- Set processing options for Maintain Business Unit Transaction Security (R95301).
- Set processing options for Business Unit Security Maintenance application (P95300).
- Revise transaction security.

Understanding How to Set Up Transaction Security

Transaction security enables you to define which transaction records a user can access, based on the business units they are associated with. Transaction security for business units is inclusive, which means that you define which transactions users can access based on the business unit to which the user ID or role is associated. To set up transaction security, you must define these items:

- Business unit type.

  A business unit type serves as a logical grouping of business units. To define it, you name it and then specify the table (typically the F0006 table) and the data item within the table that contains the business unit values.

  > **Note:** If you are setting up transaction security for an existing business unit type, use the Maintain Business Unit Security menu to add transaction security.

- Tables to include in a transaction security definition.
- Users associated with the business units.

The application that you use to set up transaction security, the Business Unit Security Maintenance application (P95300), is available in two modes: a mode that you can use for the initial transaction security setup and another mode to revise transaction security. The mode for the initial setup uses a director or wizard-like process to lead you through the P95300 application forms used to set up transaction security.

See *Setting Up Transaction Security*.

The mode to revise transaction security provides access to the same forms that are used for the initial setup, but without the wizard functionality. You can use these forms to add, update, or delete transaction security.

See *Revising Transaction Security*.

Generating Transaction Security Records

When you set up or revise transaction security, JD Edwards EnterpriseOne does not automatically enable transaction security in the software. The new or revised transaction security records must be added to the Security Workbench table (F00950). JD Edwards EnterpriseOne provides different mechanisms for updating transaction security records in the F00950 table, depending on whether you are performing an initial setup of transaction security or revising transaction security.

After you perform an initial setup, you must run the Maintain Business Unit Transaction Security batch application (R95301) to generate the transaction security records. You can set processing options for this batch application that enable you to review the records in a "proof" mode before the records are updated in the F00950 table.

See *Setting Processing Options for Maintain Business Unit Transaction Security (R95301)*.

If you are revising transaction security, you can set processing options to control how the transaction security records are updated in the F00950 table. You can set these processing options on the Maintain Business Unit Security menu, which is the EnterpriseOne menu that launches the forms used for revising transaction security.

See *Setting Processing Options for Business Unit Security Maintenance Application (P95300)*.

When you change (add, update, delete) transaction security, you must run the Maintain Business Unit Transaction Security Records (R95301) batch application for the changes to take effect.

> **Note:** Because the data in the F00950 table is cached, you must clear the cache in order for the updated security records to take affect. See *Cached Security Information*.

Setting Up Transaction Security

Access the Business Unit Security Definition Revisions form. Enter **GH9052** in the Fast Path, and then select Security Maintenance, Business Unit Security, Set-up Business Unit Security.

1. On the Business Unit Security Definition Revisions form, complete these fields in order:
   - Business Unit Type
   - Business Unit Definition Table

     Enter the table object name that contains the individual business unit values (for example, F0006).
   - Business Unit Definition Data Item

     Enter the data item in the Business Unit Definition Table that contains the unique business unit name (for example, MCU).
2. Press Tab and then click Next to continue.
3. On User/Role to Business Unit Relationships, assign the users or roles in the right panel to the appropriate business units in the left panel.

   You can search for particular business unit values and users or roles by clicking the search button next to the Business Unit Value and User/Role fields, respectively.
4. After securing users to the appropriate business units, click Next to continue.
5. On Maintain Transaction Security Tables, complete these columns in the grid:
   - Transaction table

     Enter the table name that contains the data item that you want to secure.
   - Data item

     Enter the data item of the column that you want to secure.

     You can use this form to secure multiple tables.
6. Click Next to continue.
7. On UDC Group/Set-ID/Business Unit Relationship, click Done.
8. Run the R95301 batch application.
9. Clear the workstation or web client cache

Setting Processing Options for Maintain Business Unit Transaction Security (R95301)

Processing options enable you to specify the default processing for applications and reports.

Transaction Security

These processing options are used to specify how the system processes the transaction security records.

Processing Option	Description
1. Add Transaction Security Records	Specify whether to run the report in Final mode or Proof mode. Use the Proof mode to generate a report of the transaction security records that will be updated in the Security Workbench table (F00950). Use the Final mode to update the records.
2. Add Transaction Security Records	Specify whether to add or to not add transaction security records. Values are: 1: Add 0: Do not add
3. Delete Transaction Security Records	Specify whether to delete or to not delete transaction security records. Values are: 1: Delete 0: Do not delete

Setting Processing Options for Business Unit Security Maintenance Application (P95300)

Processing options enable you to specify the default processing for applications and reports.

You can access these processing options from the EnterpriseOne Menus by right-clicking the Maintain Business Unit Security menu, and then selecting Values.

Mode

This processing option is used to specify the business unit security mode.

Processing Option	Description
1. Business Unit Security Mode	Specify whether to run the report in Director Mode (A) or Maintenance Mode (D).

Transaction Security

These processing options are used when working with business unit security in Maintenance mode only.

Processing Option	Description
1. In Maintenance mode, automatically add transaction security records.	Specify whether to automatically add transaction security records. Values are: 1: Add

Processing Option	Description
	0: Do not add
2. In Maintenance mode, automatically delete transaction security records.	Specify whether to automatically delete transaction security records. Values are: 1: Delete 0: Do not delete

Revising Transaction Security

Access the Work With Business Unit Security form. Enter **GH9052** in the Fast Path, and then select Business Unit Security, Maintain Business Unit Security.

1. On the Work With Business Unit Security form, select the business unit security type record that you want to revise.
2. To revise the users or roles associated to a business unit, from the Row menu, select Associate User/Role.
3. To revise the UDC values that are assigned to business units, from the Row menu, select UDC Groups for BU.
4. To revise a transaction table record, from the Row menu, select Transaction Tables.
5. To delete transaction security for a business unit type, select the record and then click Delete.
6. Run the R95301 batch application.
7. Clear the workstation or web client cache.

30 Upload and Download Security

Understanding Upload and Download Security

JD Edwards EnterpriseOne provides security that limits the types of files users can upload and download in EnterpriseOne. Upload security prevents users from uploading file types that might contain unknown or malicious content that can harm the system. Download security restricts users from opening files from EnterpriseOne, unless the files are system-generated files such as reports, UBE definitions, and report templates, or are files attached to media objects through the image media object queue.

Configuring Upload Security

In EnterpriseOne, there are two lists the system uses to identify the types of files that users are allowed to upload: a system-defined inclusion list and a user-defined inclusion list. Each inclusion list contains the allowed file types, which are identified by their extensions. If a file type is not in an inclusion list, it cannot be uploaded in EnterpriseOne. An administrator can modify the user-defined inclusion list.

System-Defined Inclusion List

EnterpriseOne has a system-defined inclusion list that identifies the types of files that EnterpriseOne users can upload by default. The system-defined inclusion list has a predefined extension and cannot be modified.

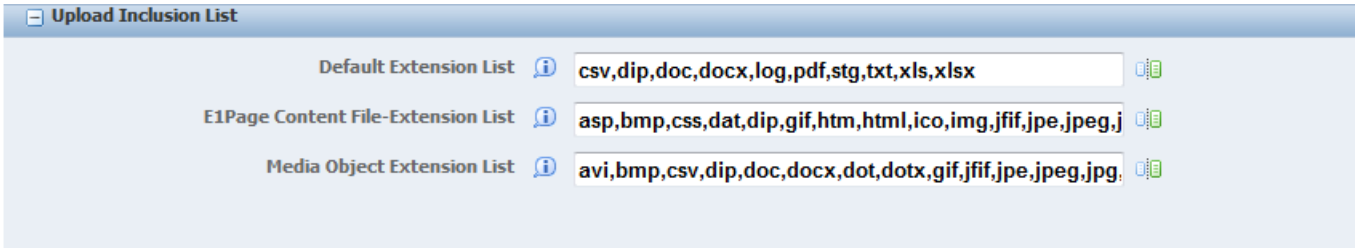
The following table lists the system-defined file types that users are allowed to upload in EnterpriseOne:

EnterpriseOne Component	Allowed File Types
EnterpriseOne Page Design— import of files for rendering the home.html	jar, zip
EnterpriseOne Pages Import	jar, zip
One View Reporting Import	jar, zip
Application grid	csv, txt, xls, xlsx, xlt, xltx
XMLP	pdf, rtf, xlf, xls, xml, xsl
MailMerge	rtf

User-Defined Inclusion List

EnterpriseOne provides a user-defined inclusion list that identifies the file types that users can upload in EnterpriseOne. The list contains a pre-defined list of file types, which administrators can modify at their discretion.

The user-defined inclusion list is made up of four settings in the `[UPLOAD]` section in the Runtime settings of the jas.ini file. You can access and update these settings in the "Upload Inclusion List" section in Server Manager, as shown in the example below:



Use the following settings to specify the file types users can upload in EnterpriseOne:

- Default Extension List (AllowDefaultFileExt in jas.ini file)

  Use this setting to identify the files types users are allowed to upload in EnterpriseOne tools other than Media Objects and EnterpriseOne Pages. The default values are csv, dip, doc, docx, dot, dotx, log, pdf, stg, txt, xls, xlsx, and xlt.

- E1Page Content File-Extension List (E1PageContentExtensionList in jas.ini file)

  Use this setting to identify the file types users are allowed to upload in EnterpriseOne pages. The default values are asp, bmp, css, dat, dip, gif, htm, html, ico, img, jfif, jpe, jpeg, jpg, js, mf, pdf, png, svg, tif, tiff, and xml.

- Mail Merge Extension List

  Use this setting to identify the file types users are allowed to upload in MailMerge Workbench. The default values are doc, docx, dot, dotx, pdf, rtf, and xml.

- Media Object Extension List (AllowMOFileExt in jas.ini file)

  Use this setting to identify the file types users are allowed to upload in Media Objects. The default values are csv, dip, doc, docx, dot, dotx, log, pdf, stg, txt, xls, xlsx, and xlt.

See the *JD Edwards EnterpriseOne Tools Server Manager Guide* for more information about modifying .ini file settings.

Additional Rules and Restrictions for Uploading Files

In addition, the following rules and restrictions apply to uploading files in EnterpriseOne:

- Files with a semicolon or colon in their name cannot be uploaded.
- File extensions cannot have more than one extension, such as `test.tst1.txt`.
- Files with no extensions can be uploaded if the user-defined inclusion list contains the value `noext`. This value is not included by default. An administrator must add it.
- Image files are scanned for a valid image file signature.
- Image files found to have embedded zip or jar files cannot be uploaded.

- When uploading zip files, EnterpriseOne scans the contents for proper file naming, allowed file types, and image file signatures.

Understanding Download Security

When downloading files from the EnterpriseOne web client on your browser, the download dialog box shows the Save and Cancel buttons, and possibly the Open button, depending on the type of file being accessed. The Open button is available only when downloading the following types of files:

- UBE, report definition, and report template.

  These files are generated by EnterpriseOne and are on a trusted server.
- Media object files that are attached as a file attachment from the image media object queue.

  You can open these file attachments because the image queue is on a trusted server and an administrator places the files in the image queue. This allows users to view these attachments (such as logs, PDFs, and so forth) in the Media Object Viewer.

Supported browsers have a built-in feature for saving files. If an EnterpriseOne user opens any of the aforementioned files in one of these browsers, the browser automatically saves the file to a "Download" folder. This enables users to open the file from the Download folder on the client machine.

31 Configuring OMW User Roles and Allowed Actions

Understanding User Roles and Allowed Actions

Note: The instructions in this chapter also apply to setting up user roles and allowed actions in the Web OMW. For more information about Web OMW, see the *JD Edwards EnterpriseOne Tools Object Management Workbench for the Web Guide*

Object Management Workbench (OMW) is the primary component of the change management system for EnterpriseOne development. OMW automates many change management activities. OMW's automation relies on an administrator who carefully configures OMW roles and allowed actions, which makes configuring these areas one of the most important EnterpriseOne configuration tasks.

These sections show the allowed user actions that Oracle recommends for each user role and the responsibility of the person in that user role, organized by the project status at which these actions should be authorized.

For status changes that initiate a transfer, the user role must be authorized to perform both the status change and transfer actions.

Note: You might want to allow the Manager and Supervisor roles to perform the same actions as the Developer role, in case the Developer cannot perform assigned duties or needs to have work verified.

For more information about OMW, see the *JD Edwards EnterpriseOne Tools Object Management Workbench Guide*

New Project Pending Review (11)

This table shows user roles and allowed actions for projects with a status of 11 (new projects pending review):

User Role	Recommended Allowed Action	Explanation
Originator	Status Change	Originator might need to advance the status to 91 - canceled. Entered in Error
Manager, Supervisor	Update Project	Change values for the project
Manager, Supervisor	Update Users	Change values for the user
Manager, Supervisor	Status Change	Advance project to the next status

Programming (21)

This table shows user roles and allowed actions for projects with a status of 21 (programming):

User Role	Recommended Allowed Action	Explanation
Developer	Add Objects	Add objects to project in order to fix or enhance
Developer	Remove Objects	Remove objects that were incorrectly added
Developer	Check Out	Check out objects from the server
Developer	Check In	Check in objects to the server
Developer	Get	Get objects from the server
Developer	Status Change	Advance project to the next status
Developer	Transfer	Transfer objects on status change

Rework-Same Issue (25)

This table shows user roles and allowed actions for projects with a status of 25 (rework-same issue):

User Role	Recommended Allowed Action	Explanation
Developer	Status Change	Change project to 21 - Programming status

QA Test/Review (26)

This table shows user roles and allowed actions for projects with a status of 26 (QA test/review):

User Role	Recommended Allowed Action	Explanation
Quality Analyst	Get	Get objects from the server
Quality Analyst	Status Change	Advance project to next status

QA Test/Review Complete (28)

This table shows user roles and allowed actions for projects with a status of 28 (QA test/review complete):

User Role	Recommended Allowed Action	Explanation
Manager, Supervisor	Update Project	Change values for the project
Manager, Supervisor	Status Change	Advance project to the next status
Manager, Supervisor	Transfer	Transfer objects on status change

In Production (38)

This table shows user roles and allowed actions for projects with a status of 38 (in production):

User Role	Recommended Allowed Action	Explanation
Manager, Supervisor	Status Change	Advance project to the next status

Complete (01)

This table shows user roles and allowed actions for projects with a status of 01 (complete):

User Role	Recommended Allowed Action	Explanation
Developer	Remove Objects	Remove objects from projects at status 91 that might have been added but not removed

Default Allowed Actions that Cannot Be Changed

These default allowed actions cannot be changed. This information is provided for reference only:

Value	Description
01	Transfer
02	Check In
03	Check Out
04	Delete
05	Add
06	Copy
08	Save
09	Restore
10	Design
11	Get
12	Remove Object from Project
13	Update a Project
16	Add Object to a Project
21	Switch Token
23	Force Release from Token Queue
30	Erase Check Out

Default Object Types

These default object types are provided for reference only:

Value	Description
01	Object Librarian objects
02	Data items
03	Versions
04	UDCs
05	Menus
06	Documentation record (SAR object)
11	Transfer record (SAR object)
12	History record (SAR object)

Setting Up User Roles

This section discusses how to:

- Modify user roles.
- Delete user roles.

Forms Used to Set up User Roles

Form Name	FormID	Navigation	Usage
Object Management Setup	W98230R	Object Management Administration menu (GH9081) then Object Management Configuration (P98230)	Access forms to configure notification subscriptions.

Form Name	FormID	Navigation	Usage
User Roles	W0004AH	In Object Management Setup, click the User Roles button.	Used to add, modify, and delete user roles.

Modifying User Roles

Access the Object Management Setup form.

1. In Object Management Setup, click User Roles.
2. Select the user role you want to modify.
3. Double-click the first field that you want to change, and modify it.
4. Repeat step 3 to make all required modifications.
5. Click Find and verify that the modifications you made appear in the list.
6. Click OK.

Deleting User Roles

Select Object Management Administration (GH9081) then Object Management Configuration (P98230)

Access the Object Management Setup form.

1. In Object Management Setup, click the User Roles button.
2. Click the cell to the left of the User Role that you want to delete.
3. Click Delete.
4. In the Confirm Delete query, click OK.
5. Repeat steps 2 through 4 to delete all desired user roles.
6. Click Find to verify that the user roles were deleted.
7. Click OK.

Setting Up Allowed User Actions

This section provides an overview of user defined codes for allowed user actions and discusses how to set up allowed user actions.

Understanding User Defined Codes for Allowed User Actions

The Allowed Actions Form lets you assign allowed actions to user roles for each object type during a specific project status. These user defined codes (UDCs) define allowed JD Edwards EnterpriseOne OMW actions involving objects:

- 01 — Transfer
- 02 — Check in
- 03 — Check out
- 04 — Delete

- 05 — Add
- 06 — Copy
- 07 — Install
- 08 — Save
- 09 — Restore
- 10 — Design
- 11 — Get
- 12 — Remove object from project
- 13 — Update the project
- 16 — Add an object to the project
- 21 — Switch tokens
- 23 — Release from token queue
- 30 — Erase check out
- 38 — Status change

For example, if you want the developer to be allowed to check in all object types when the project is at project status 21, you would enter these values in the Allowed Actions Form:

Field	Value
User Role	02 - Developer
Object Type	*ALL
System Code	System
Allowed Action	02 - Check in
Project Status	20 - Programming

Note: Before setting up allowed actions, you must add the user role to the User Roles UDC by using the User Defined Code form.

Form Used to Set Up User Actions

Form Name	FormID	Navigation	Usage
Object Management Setup	W98230R	Object Management Administration menu (GH9081) then	Access forms to configure notification subscriptions.

Form Name	FormID	Navigation	Usage
		Object Management Configuration (P98230)	
Allowed Actions	W98230G	In Object Management Setup, click the Allowed Actions button.	Used to set up user allowed actions.

Setting Up Allowed User Actions

Access the Object Management Setup form.

1. In Object Management Setup, click the Allowed Actions button.
2. Click Find to display previously defined user actions.
3. To create a blank row in which to add a definition, sort on the allowed user action to be worked on.
4. Complete one or more of the query by example (QBE) columns and click Find.
5. Scroll to a blank row at the bottom of the sorted list.
6. Complete these fields in the blank row:
   - JD Edwards EnterpriseOne OMW User Role
   - Object Type
   - Project Status
   - System Code
   - System Code Reporting
   - Action

   > **Note:** You can enter *ALL in any field except User Role. Typing *ALL in a field indicates that the user role chosen can work with all object types, project statuses, or actions.

   After you complete a row, a new blank row appears.
7. Repeat this procedure until all allowed user actions are set up.
8. Click OK.

32 Configuring EnterpriseOne Security Auditing

Overview of EnterpriseOne Auditing Tools

Oracle recommends that you regularly run security reports to review existing security records and ensure that users have the appropriate level of access to system objects and data. EnterpriseOne contains a set of reports and tools than enable you to audit security records and other security-related information. The auditing mechanisms include:

- Security Analyzer Reports
  Run these reports to review the sign-in security records by data source and by user or role.
- Security Workbench Records Reports
  Run these reports to review the object security records by object type and user or role.
- Auditing Tools for Administering 21 CFR Part 11 Auditing
  Oracle's JD Edwards EnterpriseOne auditing and electronic signature tools provide a solution to the Food and Drug Administration's (FDA) acceptance of electronic signatures and audit records for FDA-required records such as product submissions, batch records, and complaints. These tools enable your organization to comply with the FDA 21 CFR Part 11 regulation for submitting electronic records. See the *JD Edwards EnterpriseOne Tools Auditing Administration Including 21 CFR Part 11 Administration Guide* for instructions on how to administer auditing for 21 CFR Part 11.

Running a Security Analyzer Report

This section contains the following topics:

- *Understanding the Security Analyzer Report*
- *Form Used to Run a Security Analyzer Report*
- *Running the Security Analyzer by Data Source Report (R98OWSECA)*
- *Running the Security Analyzer by User or Group Report (R98OWSECB)*

Understanding the Security Analyzer Report

This process generates two separate reports that provide you with an analysis of JD Edwards EnterpriseOne security. The first report is the Security Analyzer by Data Source (R98OWSECA); it is organized and sorted by data source. A blank data source means that security for the System User ID is applicable to all data sources. The Security Analyzer by Data Source report is based on data that it reads from the F98OWSEC table.

The second report is the Security Analyzer by User or Group (R98OWSECB); it is organized by user or role. The Security Analyzer by User or Role report is also based on data that it reads from the F98OWSEC table.

Form Used to Run a Security Analyzer Report

Form Name	FormID	Navigation	Usage
Work With Batch Versions - Available Versions	W98305A	Report Management (GH9111), Batch Versions (P98305)	Run the Security Analyzer by Data Source (R98OWSECA) and Security Analyzer by User or Group (R98OWSECB) reports.

Running the Security Analyzer by Data Source Report (R98OWSECA)

This report presents security analysis information for each data source, each user ID, and each role. The report is sorted by data source and then by user ID. This columnar data appears in the report:

- Data Source

  The data source to which the user is secured. Blank indicates all data sources.
- User ID
- User / Role

  An identification code for a user profile.
- System User ID

  The actual user that JD Edwards EnterpriseOne uses to connect to the DBMS that you specified as the data source. This system user must match the user value that is defined in the DBMS.
- Change Frequency

  The number of days before the system requires that a user change their password. This data can be set by individual user ID or by role.
- Source Password Changed

  The date when a user's password was last changed.
- Invalid Signons

  The number of invalid sign-in attempts by a user. If the retry count value exceeds the number of allowed attempts, the user profile is disabled.
- Allowed Attempts

  The number of sign-in attempts that a user can make before that user profile is disabled.

- User Status

  A value that indicates whether the user can sign in to JD Edwards EnterpriseOne. Values are **01** (enabled) and **02** (disabled).

- Status

  The display status of the User Status field.

Access the Work With Batch Versions - Available Versions form to run the Security Analyzer by Data Source Report (R98OWSECA).

1. Select a version and then click Select.

   The default version is XJDE0001. It creates a report for all user IDs for all data sources.
2. On the Version Prompting form, click Submit.
3. On the Report Output Destination form, select any of these options:
   - On Screen
   - To Printer
   - Export to CSV
4. If desired, select the OSA Interface Name option and enter a name in the box that appears.

Running the Security Analyzer by User or Group Report (R98OWSECB)

The Security Analyzer by User or Group Report (R98OWSECB) report presents security analysis information for each user ID, each group, and each data source. The report is sorted either by user ID or user group, depending on which processing option you select. This columnar data appears in the report:

- User ID
- Role
- Password Change Frequency

  The number of days before a user must change their password. This data can be set by individual user ID or by group.

- Data Source

  The data source to which the user is secured. A blank indicates all data sources.

- System User

  The actual user that the software uses to connect to the DBMS that you specified as the data source. The system user that is defined here must match the user value that is defined in the DBMS.

Access the Work With Batch Versions - Available Versions form to run the Security Analyzer by User or Group Report (R98OWSECB).

1. Select a version and click Select.

   The default version is XJDE0001. It creates a report for all user IDs for all data sources.

   By default, the XJDE0001 version has the processing option for this report set to **1.** This option generates a report by user ID.

   To generate a report by role, you can prompt for processing options and then, on the User Setup tab, change the value to **2.**
2. On the Version Prompting form, click Submit.
3. Complete the processing options as necessary, and then click OK.
4. On Report Output Destination, select any of these options:
   - On Screen
   - To Printer
   - Export to CSV
5. If desired, select the OSE Interface Name option and type a name in the field that appears.

Running Security Workbench Records Reports

This section provides an overview of the Security Workbench Records reports and discusses how to:

- Run the Security Audit Report by Object version (R009501, XJDE0001).
- Run the Security Audit Report by User version (R009502, XJDE0001).
- Run the Security Audit Report by Role version (R009502, XJDE0002).

Understanding the Security Workbench Records Reports

JD Edwards EnterpriseOne provides two Security Workbench Records reports—Security by Object (R009501) and Security by User/Role (R009502)—that you can run to review the current security records by object type and user or role. The Security Workbench Records reports list security records for these objects:

- Interactive and batch applications.
- Tables (rows and columns).
- Published business services.

Before choosing which report to run, you should consider the data that you want the report to produce. Run the Security by Object report (R009501) to generate a report that lists the security records based on a particular object, object type, or product code. You can refine the data selection for this report to list only records for a particular user ID, role, or a combination of user ID and role. Run the Security by User/Role report (R009502) to generate a report that lists all the application, row, column, and published business service security records for a particular user ID, role, or *PUBLIC.

Each report contains processing options that you can use to define the output of the report. Along with the processing options, you can use the Data Selection form in the Batch Version application (P98305W) to further refine the data that the report produces.

Each security record in the report indicates the level of security, or type of security, that is applied to the object. For application security, each record indicates if a user or role has permission to install, run, or both install and run the application. For row security, each record indicates if view, add, change, or delete security have been applied. For column security, each record indicates if view, add, or change security have been applied. For published business service security, each record indicates whether a user or role has access to the published business service object.

How you set up your report determines how readily you can find gaps in your security plan. For example, if you have a highly sensitive application and you want to ensure that only the appropriate users have access to it, you can refine the R009501 report (Security Audit Report by Object) to list only the security records for that particular application.

Example of Security by Object Report (R009501)

This example shows the results of running the R009501 report. The report has been set up to list all the security records for the P00950 application.

R009501

Worldwide Company

Security Workbench Records by Object

Object Name: P00950 Security Workbench

Application Security

User/ Role	Application/Form Name	Version	Run	Install
*PUBLIC	P00950		N	N
AJ5596202	P00950		Y	Y
AR6870955	P00950		Y	Y
BS857012	P00950		Y	Y
CD6815454	P00950		Y	Y
DC17347	P00950		Y	Y
DG5416259	P00950		Y	Y
GA5807541	P00950		Y	Y
GB5915023	P00950		Y	Y
IC8812281	P00950		Y	Y
IC8866773	P00950		Y	Y
IO5634133	P00950		Y	Y
JN7189900	P00950		Y	Y
JR5416873	P00950		Y	Y
JR5984977	P00950		Y	Y
KC5521825	P00950		Y	Y

Example of Security Audit Report by User (R009502, XJDE0001)

This example shows the results of running the Security Audit Report by User version of the R009502 report. The report lists the security records for a particular user in order of application, row, and then column. This example shows only the first page of the report, which lists the application security records for the user ID.

R009502 Worldwide Company 1/4/2006 12:56:41
Security Workbench Records by User/Role Page - 1

User ID: KC5731873
Application Security

Login Role	Application/Form Name	Version	Run	Install	Derived From User/Role
*ALL	P0082		Y	Y	KC5731873
*ALL	P00945		Y	Y	KC5731873
*ALL	P00950		Y	Y	KC5731873
*ALL	P4112		Y	Y	KC5731873
*ALL	P45520		N	Y	*PUBLIC
*ALL	P559861		Y	Y	KC5731873
*ALL	P55CRAP1		N	N	*PUBLIC
*ALL	P55GWYN		N	N	*PUBLIC
*ALL	P55OMWFX		Y	Y	KC5731873
*ALL	P7308		N	N	*PUBLIC
*ALL	P87030		Y	Y	KC5731873
*ALL	P87SAR		Y	Y	KC5731873
*ALL	P9060		N	N	*PUBLIC
*ALL	P91300		Y	Y	KC5731873
*ALL	P9220		Y	Y	KC5731873
*ALL	P95012		Y	Y	KC5731873
*ALL	P95921		Y	Y	KC5731873
*ALL	P960092		N	N	*PUBLIC
*ALL	P960092B		N	N	*PUBLIC
*ALL	P9601		Y	Y	OWTOOL

Example of Security Audit Report by Role (R009502, XJDE0002)

This example shows the results of running the Security Audit Report by Role version of the R009502 report. The data selection of the report has been defined to list security records for the OWTOOL role. This example shows the third page of the report, which lists the row and column security records for the OWTOOL role.

R009502 Worldwide Company 1/4/2006 13:00:30

Security Workbench Records by User/Role Page - 3

Row Security	Login Role	Table Name	Alias	From Value	Thru Value	View	Add	Change	Delete	Derived From User/Role
	OWTOOL	F98221	OMWUR	06	06	Y	Y	Y	Y	OWTOOL
	OWTOOL	F986101	DATP	Business Data - PDEVDATA	Business Data - PDEVDATA	Y	N	N	N	*PUBLIC
	OWTOOL	F986101	OBNM	F00942	F00942	Y	N	N	N	*PUBLIC
	OWTOOL	F986101	OBNM	F00950	F00950	Y	N	N	N	*PUBLIC
	OWTOOL	F986101	OBNM	F98223	F98223	Y	N	N	N	*PUBLIC
	OWTOOL	F986101	OBNM	F98225	F98225	Y	N	N	N	*PUBLIC
	OWTOOL	F986101	OBNM	F986101	F986101	Y	N	N	N	*PUBLIC
	OWTOOL	F986101	UGRP	*PUBLIC	*PUBLIC	Y	N	N	N	*PUBLIC
	OWTOOL	F986167	USER	*PUBLIC	*PUBLIC	Y	N	N	N	*PUBLIC

Column Security	Login Role	Table Name	Alias	View	Add	Change	Derived From User/Role
	OWTOOL	F0092	AN8	Y	N	N	*PUBLIC
	OWTOOL	F0092	UGRP	Y	N	N	*PUBLIC
	OWTOOL	F00941	RLS	Y	Y	N	*PUBLIC
	OWTOOL	F00942	RLS	Y	Y	N	*PUBLIC
	OWTOOL	F00942	SERSHP	Y	Y	N	*PUBLIC
	OWTOOL	F0111	AN8	Y	Y	N	*PUBLIC
	OWTOOL	F4209	MCU	Y	Y	N	*PUBLIC
	OWTOOL	F4211	LOTN	N	N	N	*PUBLIC

Run the Security Audit Report by Object Version (R009501, XJDE0001)

Access the Work With Batch Versions - Available Versions form. To do so, enter **P98305W** in the Fast Path.

1. In the Batch Application field, enter **R009501** and click the Find button.
2. Select the Security Audit Report by Object version.

3. To define processing options for the report, select Processing Options from the Row menu, and then complete the processing options as appropriate:
   - User ID or Role (optional)

     Enter a user ID or role to refine the report to generate only records based on that particular user ID or role.
   - Report on Application Security

     Leave blank if you want the report to include application security records. Enter **1** to exclude application security records.
   - Report on Row Security

     Leave blank if you want the report to include row security records. Enter **1** to exclude row security records.
   - Report on Column Security

     Leave blank if you want the report to list application security records. Enter **1** to exclude application security records.
   - Report on Published BSSV Security

     Leave blank if you want the report to list published business service security records. Enter **1** to exclude published business service security records.

     > **Note:** In addition, to generate a report that displays published business service security records, you need to add an additional condition in the Data Selection form, as discussed below.
4. On the Work With Batch Versions - Available Versions form, click Select.
5. On the Versions Detail form, select the Data Selection check box and click the Submit button.
6. On the Data Selection form, you can add a condition to filter on a particular object, object type, or product code.

   If the processing option is set to list published business service security records, you must add the following condition after the default `Where` condition:

   ```
   And BC Source Language (F9860) (SRCLNG) [BC] is equal to "SBF"
   ```
7. Click the OK button.
8. On the Printer Selection form, define the location for the output of the report and then click OK to submit it.

Run the Security Audit Report by User Version (R009502, XJDE0001)

Access the Work With Batch Versions - Available Versions form. To do so, enter **P98305W** in the Fast Path.

1. In the Batch Application field, enter **R009502** and click the Find button.
2. Select the Security Audit Report by User version.
3. To define processing options for the report, select Processing Options from the Row menu, and then complete the processing options as appropriate:
   - Role (optional)

     To refine the report to generate only records based on a particular role of the user, enter a role.
   - Report on Application Security

Leave blank if you want the report to include application security records. Enter **1** to exclude application security records.

- Report on Row Security

  Leave blank if you want the report to include row security records. Enter **1** to exclude row security records.

- Report on Column Security

  Leave blank if you want the report to list column security records. Enter **1** to exclude column security records.

- Report on Published BSSV Security

  Leave blank if you want the report to list published business service security records. Enter **1** to exclude published business service security records.

4. On the Work With Batch Versions - Available Versions form, click Select.
5. On the Versions Detail form, select the Data Selection check box and click the Submit button.
6. On the Data Selection form, use the User ID left operand to define the user ID that you want the report to list security records for.
7. Click OK.
8. On the Printer Selection form, define the location for the output of the report and then click OK to submit it.

Run the Security Audit Report by Role Version (R009502, XJDE0002)

Access the Work With Batch Versions - Available Versions form. To do so, enter **P98305W** in the Fast Path.

1. In the Batch Application field, enter **R009502** and click the Find button.
2. Select the Security Audit Report by Role version.
3. To define processing options for the report, select Processing Options from the Row menu, and then complete the processing options as appropriate:
   - Role (optional)

     Do not use this option for this report. Instead, enter the role in the Data Selection form.

   - Report on Application Security

     Leave blank if you want the report to include application security records. Enter 1 to exclude application security records.

   - Report on Row Security

     Leave blank if you want the report to include row security records. Enter 1 to exclude row security records.

   - Report on Column Security

     Leave blank if you want the report to list application security records. Enter 1 to exclude application security records.

   - Report on Published BSSV Security

     Leave blank if you want the report to list published business service security records. Enter **1** to exclude published business service security records.
4. On the Work With Batch Versions - Available Versions form, click Select.
5. On the Versions Detail form, select the Data Selection check box and click the Submit button.

6. On the Data Selection form, use the User ID left operand to define the role that you want the report to list security records for.
7. Click OK on the Data Selection form.
8. On the Printer Selection form, define the location for the output of the report and then click OK to submit it.

Running a Report that Lists Published Business Service Security Records

You can use the Security Workbench Records reports to generate a list of published business service security records by object, user, or role. However, before you run the report, you must use the Data Selection form to specify the published business service object type.

Access the Work With Batch Versions - Available Versions form. To do so, enter **P98305W** in the Fast Path.

1. In the Batch Application field, enter either **R009501**or **R009502** and click the Find button.
2. Select the version of the report that you want to run.
3. On the Work With Batch Versions - Available Versions form, click Select.
4. On the Versions Detail form, select the Data Selection check box and click the Submit button.
5. On the Data Selection form, enter these conditions and then click OK:

   ```
   Where BC Object Type (F9860) (FUNO) is equal to "BSFN"
   And BC Source Language (F9860) (SRCLNG) [BC] is equal to "SBF"
   ```
6. On the Printer Selection form, define the location for the output of the report and then click OK to submit it.

33 Appendix A - DB Password Encryption

DB Password Encryption

Note: This appendix has been updated in its entirety for JD Edwards EnterpriseOne Tools Release 9.1 Update 3. THIS APPENDIX IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. This publication could include technical inaccuracies or typographical errors. This publication does not make recommendations, implied or actual. It provides guidelines; however, due the wide variety of networking, hardware and software configurations found in JD Edwards EnterpriseOne installations, no guarantees can be made that specific results are achievable in any particular installation. Changes are periodically added to the information herein. These changes will be incorporated in new editions of the publication. Oracle may make improvements and changes at any time to the products and programs described in this publication.

This appendix is intended for an administrator who is going to apply the EnterpriseOne Tools Release at the customer site. It is assumed that the reader has knowledge of JD Edwards EnterpriseOne and CNC technology.

Understanding the Problem

Starting with the JD Edwards EnterpriseOne Tools 9.1.3, the algorithm used to encrypt EnterpriseOne passwords has been changed to a one-way hash. This enhancement addresses the vulnerability that exists when storing passwords in the database and the associated installation/migration issues. The solution updates the passwords stored in the database to a higher encryption standard.

Converting Security

This EnterpriseOne Tools 9.1.3 enhancement improves the security of passwords stored in the database by replacing existing password encryption with one-way hash encryption. This conversion from the old encryption to the one-way hash encryption occurs in these instances:

- When a user login occurs AND the following setting is in the Enterprise Server jde.ini file:

  ```
  [SECURITY]

  ONTHEFLYMIGRATION=1
  ```

  During the user login, the security kernel checks whether the user record in the security table is stored using the old encryption. If it is stored using the old encryption, the kernel updates all user records in security tables to one-way hash encryption. Since this happens only once, the impact to the login process is minimal.

  Note: This setting is not available in Server Manager. An administrator must add this setting to the Enterprise Server jde.ini setting to enable one-way hash encryption for existing user passwords.

- When the administrator adds a user to EnterpriseOne.

When the administrator adds a user record, a message is sent to the security kernel for processing. The security kernel encrypts the password using one-way hash encryption and inserts the user records in the security tables.

In summary, starting with EnterpriseOne Tools 9.1.3, new users added to EnterpriseOne will have their passwords encrypted with one-way hash. For existing users, EnterpriseOne will use one-way hash for password encryption only if you add the ONTHEFLYMIGRATION=1 setting to the Enterprise Server jde.ini file.

Understanding the Impacted Components

Starting with EnterpriseOne Tools 9.1.3, the security kernel has been updated to detect the old encryption and to re-encrypt records using one-way hash encryption.

The EnterpriseOne Tools Release 9.1.3 must be deployed on all Enterprise Servers sharing the same F98OWSEC table.

Configuring New Encryption

After this update is installed on Enterprise Servers, the security kernel stores passwords in the security tables using one-way hash encryption, and there is no way to disable the encryption for new EnterpriseOne users or revert to the old configuration.

Preparing for Installation

Before starting the pre-installation process, make sure you create a backup copy of the F98OWSEC table, for example F98OWSECBK. This backup copy can be in the same data source or a different one. You only use this backup in the event that you need to roll back the EnterpriseOne Tools Release.

Special Instructions for Multiple Enterprise Servers Sharing the Same F98OWSEC Table

If you have more than one EnterpriseOne Enterprise Server sharing the same F98OWSEC table, you have to update all of them to EnterpriseOne Tools 9.1 Update 3 to support one-way hash encryption.

If you do not want to update all EnterpriseOne Enterprise Servers to EnterpriseOne Tools 9.1 Update 3, then you need to create two Security Server data sources: one for Enterprise Servers on Tools 9.1 Update 3 and one for EnterpriseOne servers on a release below Tools 9.1 Update 3. In this scenario, only the Enterprise Servers on Tools 9.1 Update 3 will support one-way hash encryption.

Creating a Separate Security Server Data Source

If you have multiple Enterprise Servers sharing the same F98OWSEC table and you are not updating all of them to Tools 9.1 Update 3, create two Security Server data sources:

- One for Enterprise Servers on Tools 9.1 Update 3 (and above).
- One for Enterprise Servers on releases below Tools 9.1 Update 3.

Note: If you are not using multiple Enterprise Servers (including multiple foundation) that share the same F98OWSEC table on different EnterpriseOne Tools releases, your existing data source is sufficient.

Configuring these data sources helps avoid data conflicts due to overlap between new and old Enterprise Servers.

The following task describes how to copy security tables to a new data source. These tables are used as a secondary location to support the one-way hash encryption.

Complete the following steps BEFORE installing the EnterpriseOne Tools Release.

CAUTION: Do not create any OCM mappings (client or server) that point to the newly created data source. Doing so will result in system errors.

To copy security tables to a new data source:

1. Log on to the Deployment Server in the appropriate environment.
2. Create a new data source.
3. Open OMW and copy all the tables in the Security data source to the new data source.

The new client and server data source must contain a copy of the following tables from the System-910 or System-900 data source: F0092, F00921, F00927, F0093, F00941, F9312, F98OWPU, and F98OWSEC. See *"Understanding and Setting Up Data Sources" in the JD Edwards EnterpriseOne Tools System Administration Guide* for instructions on how to use the Data Sources application (P986115) to create a new client and server data source.

For each EnterpriseOne Enterprise Server on Tools release 9.1.3.0 or above, set the DataSource setting in the SECURITY settings to the new client and server data source.

For each EnterpriseOne Enterprise Server on Tools release prior to 9.1.3.0, set the DataSource setting in the SECURITY settings to "System - 910" or "System - 900".

Note: *"Copying Tables" in the JD Edwards EnterpriseOne Tools Table Design Guide* for more information about using the Object Management Workbench and Table Design Aid to copy tables.

Updating JD Edwards EnterpriseOne

To complete this update, you must update all the servers and workstations in your EnterpriseOne environment. Complete the tasks below that are relevant to your configuration when installing EnterpriseOne Tools Release 9.1.3 or above.

Note: For information about installing the EnterpriseOne Tools Release on the Deployment Server, see the *JD Edwards EnterpriseOne Deployment Server Reference Guide* for your platform located at: `http://docs.oracle.com/cd/E61420_01/index.htm`

The EnterpriseOne Tools Release must be deployed on all Enterprise Servers sharing the same F98OWSEC table as well as all clients that communicate with these servers.

1. Deployment Server
   Follow the instructions in the "Installing a Tools Release on the Deployment Server" section of the *JD Edwards EnterpriseOne Deployment Server Reference Guide* for your platform located at:
   `http://docs.oracle.com/cd/E61420_01/index.htm`
2. Enterprise Server
   a. Follow the instructions in section *"Change a Managed EnterpriseOne Software Component" in the JD Edwards EnterpriseOne Tools Server Manager Guide* to install the EnterpriseOne Tools Release to the appropriate host installation.
   b. If you copied the tables in the Security data source to a new data source during the pre-installation process, update the jde.ini file on the Enterprise Server with the following changes before starting the network services:
   ```
   [SECURITY]
   DataSource=<new data source name>
   ```
   This is the new data source defined in the pre-installation process.
   c. Verify that you can run PORTTEST successfully.
3. To install the HTML Server changes, follow the instructions in the *JD Edwards EnterpriseOne HTML Server Reference Guide* for your platform located here:
   `http://docs.oracle.com/cd/E61420_01/index.htm`
4. Deploy a client package for the EnterpriseOne Tools Release:
   a. Modify the Deployment Server update package created by the ESU process (see the Deployment Server section above). Create the foundation to include the EnterpriseOne Tools Release 9.1.3 or above.
   b. Make sure this package is defined for clients.
   c. Build and deploy the package to all workstations.
5. Run the web client and Microsoft Windows client to make sure users can log in.
6. Run the security administration application to make sure a new user can be added and passwords for existing users can be modified.

Reviewing the Installation

Review the following considerations after the system is updated:

1. If the setting `ONTHEFLYMIGRATION=1` is in the Enterprise Server jde.ini file, user records are encrypted with one-way hash encryption when the user logs in. There is no way to disable the encryption or revert back to the old security configuration.
2. There is no procedure to rollback user records to the old encryption nor is there a procedure for converting all user records to the new encryption. *The backup copy of the F98OWSEC table can be used to reset the user data.*
3. If the customer has multiple Enterprise Servers at different EnterpriseOne Tools Release levels, make sure each of them is pointing to the correct security data sources:
   - If an Enterprise Server running an older EnterpriseOne Tools Release accesses data encrypted using one-way hash encryption, authentication will fail and users will not be able to log in.

- If an EnterpriseOne user signs into an Enterprise Server running EnterpriseOne Tools Release 9.1.3 or above, and the user's password is encrypted using the old encryption, the Enterprise Server updates the user's records in the Security tables to the one-way hash encryption. This only occurs if the setting `ONTHEFLYMIGRATION=1` is in the Enterprise Server jde.ini.
- If a new EnterpriseOne user is added using EnterpriseOne Tools Release 9.1.3 or above, the new user password is stored using one-way hash encryption. Consequently, this user will NOT be able to sign in to older EnterpriseOne Tools Releases that share the same F98OWSEC table.
- If a new EnterpriseOne user is added using an EnterpriseOne Tools Release prior to 9.1.3, the new user password is stored using the old encryption. Therefore, this user can sign in to any EnterpriseOne Tools Release sharing the same F98OWSEC table, as long as the Enterprise Server jde.ini files do NOT include the setting `ONTHEFLYMIGRATION=1`.

4. If the customer has multiple Enterprise Servers at different EnterpriseOne Tools Release levels, a dual maintenance procedure for users and passwords is required. Once all the foundations are running an EnterpriseOne Tools Release 9.1.3 or above:
   a. The jde.ini setting for SECURITY Data Source can be changed to point to the same data source for all servers running EnterpriseOne Tools Release 9.1.3 or above.
   b. Save the backup copy of the F98OWSEC table in case you need to roll back the EnterpriseOne Tools Release as described in *Rolling Back the Software*..

Rolling Back the Software

The improved encryption will be part of all future EnterpriseOne Tools Releases and it can not be disabled. If you decide to roll back to a previous EnterpriseOne Tools Release, complete these steps:

1. Follow the installation instructions to roll back the Enterprise Server and client workstations.
2. Restore the backup F98OWSEC table in the appropriate data source from the backup copy (for example F98OWSECBK).
3. Change the INI setting for SECURITY data source to point to the correct data source with the restored F98OWSEC table.
4. Run PORTTEST on the Enterprise Server to make sure users can log in.

Copyright

```
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
```

```
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```

34 Appendix B - Creating a JD Edwards EnterpriseOne LDAP Configuration for OID

Understanding JD Edwards EnterpriseOne LDAP Configuration for OID

This appendix is a supplement to the *Enabling LDAP Support in JD Edwards EnterpriseOne* chapter in this guide. Use the settings detailed in this appendix as a reference when creating an LDAP configuration for Oracle Internet Directory (OID).

OID is an LDAP compliant directory service. You can configure JD Edwards EnterpriseOne to use OID as the LDAP server. This enables administrators to use the directory service to manage user information such as user IDs, passwords, and user-role relationships.

> **Note:** This section does not contain all of the steps for creating an LDAP configuration, only specific values that are required for setting up an LDAP configuration for OID.

When you configure OID as the LDAP server, the settings that you configure depend on how you plan to use OID, which can include these scenarios:

- Managing only user IDs and passwords.
- Managing user-role relationships in addition to user IDs and passwords.
- Using Secure Socket Layer (SSL).
- Using the User Profile Self-Service application (P0092SS).

> **Note:** *Enabling LDAP Support in JD Edwards EnterpriseOne*. *Oracle Internet Directory Administrator's Guide* located at: `http://docs.oracle.com/cd/E12839_01/admin.1111/e10029/toc.htm`

Adding OID to the List of LDAP Server Types

Before you can create an LDAP configuration for OID, you must manually add OID as an option in the LDAP Server Type field of the LDAP Server Configuration Workbench application (P95928). To do so, use the User Defined Code application (P0004A) to add a UDC for OID.

Access the Work With User Defined Codes form. In JD Edwards Solution Explorer, enter **UDC** in the Fast Path.

1. Complete these fields and click **Find**:

Field	Value
Product Code	**95**

Field	Value
User Defined Codes	**LS**

2. Click **Add**.
3. On the User Defined Codes form, scroll to the last empty row of the detail area.

> **Note:** Be sure to add the new code on the *last* detail row so that you do not inadvertently overwrite a blank code, which might appear in the first detail row. A blank code might have only a period in the Description field.

4. Complete these fields and click **OK**:

Field	Value
Codes	**OID**
Description 1	**Oracle Internet Directory**

Creating an LDAP Configuration for OID

Use this section as a reference for creating an LDAP configuration.

See *Creating an LDAP Configuration*.

When you create an LDAP configuration for OID, on the LDAP Server Information form, you must select OID in the LDAP Server Type field.

Configuring the LDAP Server Settings for OID

Use the OID settings in this section as a reference for configuring the LDAP server settings.

See *Configuring the LDAP Server Settings*.

The values in the tables are variables and will differ depending upon your configuration.

Configure these attributes:

Attribute	Value
USRSRCHBAS	cn=Users,dc=jdedwards,dc=com

Attribute	Value
USRSRCHFLT	objectclass=inetOrgPerson
USRSRCHSCP	subtree

If roles are enabled in LDAP, configure these attributes:

Attribute	Value
ROLSRCHBAS	cn=Groups,dc=jdedwards,dc=com
ROLSRCHFLT	objectclass=groupofUniqueNames
ROLSRCHSCP	subtree

If you are using SSL with LDAP server, configure these attributes as well:

Attribute	Value
SSLPORT	636
CERTDBPATH	c:\certdbdir (Directory path for cert7.db)

If you are using the user profile self-service application for the Manufacturing Sourcing module, configure these settings:

Attribute	Value
USRADDLOC	cn=Users, dc=jdedwards,dc=com
USRCLSHRCY	top,person,organizationalperson,inetOrgPerson,orcluser,orcluserv2
ROLADDLOC	cn=Groups,dc=jdedwards,dc=com

Configuring LDAP to JD Edwards EnterpriseOne Enterprise Server Mappings for OID

Use the OID settings in this section as a reference for configuring LDAP to JD Edwards EnterpriseOne enterprise server mappings.

See *Configuring LDAP to EnterpriseOne Enterprise Server Mappings*.

The values in the tables are variables and will differ depending upon your configuration.

Configure these attributes:

Attribute	Value
E1USRIDATR	uid
USRSRCHATR	uid
EUSRIDATR	uid

If roles are enabled in LDAP, configure these attributes:

Attribute	Value
ROLNAMEATR	cn
ROLSRCHATR	uniquemember

If you are using the user profile self-service application for the Manufacturing Sourcing module, configure these settings:

Attribute	Value
CMNNAME	cn
SURNAME	sn
PASSWORD	userPassword
OBJCLASS	objectClass

35 Appendix C - JD Edwards EnterpriseOne Cookies

Web Runtime Cookies

This table lists the web runtime cookies that the HTML Server sends to a web browser when running JD Edwards EnterpriseOne web applications.

JD Edwards EnterpriseOne Web Runtime Cookie	Purpose	Life Span	Turn ON/OFF
com_jdedwards_LastLayout	This cookie stores the Portal Workspace (WORKSPACEID) that was last accessed by a user (USERID). **Note:** This cookie is only applicable to Portal users.	The life span of the cookie is one year.	You cannot turn off this cookie.
com_jdedwards_CSN	This cookie stores the information to implement critical state functionality for the HTML Client Component running inside the Portal.	10000 milliseconds.	You cannot turn off this cookie.
advancedState	This cookie stores the information about whether to display the Environment and Role fields on the JD Edwards EnterpriseOne sign-in screen.	Seven days.	This cookie is created only if the DisplayEnvironment property defined in the [LOGIN] section of the JAS.INI is not set to "HIDDEN".
jdeLoginCookie	This cookie stores the username, password, role, language code and rtlLayout information about a user's login in an encrypted format.	The life span of the cookie depends on the value of CookieLifeTime property defined in the [SECURITY] section of the JAS.INI file. If this property is not defined, then by default, this cookie's life span is set to seven days.	This cookie is not created if the UseLogonCookie property defined in the [SECURITY] section of the JAS.INI is set to false. The system does not create this cookie by default.
AutoPopulate	This cookie stores a user's preference of whether to auto populate the grid on a form. A user can turn	The life span of the cookie one year.	You cannot turn off this cookie.

JD Edwards EnterpriseOne Web Runtime Cookie	Purpose	Life Span	Turn ON/OFF
	the autopopulate grid option on/off by using the AutoPopulate option in the Tools menu on a form.		
maxLogLength	This cookie determines the maximum number of javascript debug statements that can be logged using JSMonitor.log() API. The default value for this cookie is 15. A developer can turn on the logging by clicking the Enable JSMonitor button after pressing Ctrl+D.	This cookie never expires.	You cannot turn off this cookie.

36 Appendix D - Default Database User Accounts

Default Database User Accounts

The following list contains the default database accounts created and used by JD Edwards EnterpriseOne 9.0:

- APPLEAD
- TESTCTL
- JDEDBA
- DV900
- PD900
- PRODUSER
- CRPCTL
- PRODCTL
- PRODDTA
- TESTDTA
- JDE
- DEVUSER
- CRPDTA
- PS900
- PY900
- DD900
- SVM900
- SY900
- OL900
- PD900DTA
- PS900CTL

37 Glossary

access provisioning

The process of setting up user and role profiles in EnterpriseOne for sign-in security (authentication) and authorization security.

add mode

A condition of a form that enables users to input data.

authentication

The process of verifying that users signing into EnterpriseOne are valid EnterpriseOne users.

authorization

The process of granting or denying users access to EnterpriseOne applications, features, data, and data sources. In EnterpriseOne, most authorization security is applied at the object level through the Security Workbench.

data encryption

The process of transforming information into code so that it cannot be read by a third party system. EnterpriseOne encrypts user passwords stored in the database.

data masking

Customizing a field so that specified characters are embedded in place of sensitive data that appears in applications. This prevents sensitive data from being displayed to unauthorized users.

data privacy

In EnterpriseOne, Address Book data security enables you to restrict users from viewing Address Book information that is determined as private, personal data.

developer security

Security that determines the actions that developers can perform when customizing or developing EnterpriseOne applications in Object Management Workbench (OMW). Actions can include checking out and checking in objects, promoting objects, transferring objects, removing objects, and so forth.

object-level security

A type of authorization security that enables you to secure specific objects within JD Edwards EnterpriseOne such as applications, forms, and various other EnterpriseOne features. Object-level security provides flexibility with applying security and a higher level of security integrity.

power form

Web-only application forms that enable users to view multiple, interrelated views of data, grids, and tab pages on one form and to pass logic between them.

*PUBLIC

A special ID within EnterpriseOne that automatically includes all users within it. This option controls security for all users who are designated by ID type ***PUBLIC** in the User or Role field.

published business service

EnterpriseOne service level logic and interface. A classification of a published business service indicating the intention to be exposed to external (non-EnterpriseOne) systems.

secure by default

A security model that assumes that a user does not have permission to execute an object unless there is a specific record indicating such permissions.

Secure Socket Layer (SSL)

A security protocol that provides communication privacy. SSL enables client and server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

security overrides

Security records that operate as exceptions to existing security records. Security overrides specify that users are *unsecured* from an EnterpriseOne object. In other words, security overrides allow users access to a particular object, even if another security record in the system specifies that access is not allowed.

security workbench

An application that enables you to secure JD Edwards EnterpriseOne objects, such as applications, forms, rows, tabs, and so on. It stores all objects security records in the F00950 table.

serialize

The process of converting an object or data into a format for storage or transmission across a network connection link with the ability to reconstruct the original data or objects when needed.

subform

A subform is a control designed for use on a power form or another subform. Power forms can contain several subforms, so a single power form with multiple subforms enables users to see multiple data views.

terminal server

A server that enables terminals, microcomputers, and other devices to connect to a network or host computer or to devices attached to that particular computer.