# Oracle® Essbase

## Essbase Independent Deployment

Release 21
F30039-19
May 2025

ORACLE

Oracle Essbase Essbase Independent Deployment, Release 21

F30039-19

# Contents

## 11 Troubleshooting

# Accessibility and Support

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.

1

# Get Started with Oracle Essbase Installation and Maintenance

Use this documentation to install, configure, and maintain Oracle Essbase.

For general product information about getting started with Essbase and its product features, see Getting Started with Oracle Essbase documentation.

**Topics:**



## Components and Terminology

Oracle Essbase incorporates powerful architectural features to handle a wide range of analytic applications across large multi-user environments. This offering of Essbase is available as part of independent deployments as a powerful platform with robust new features.

Architecture — Essbase architecture includes a middle-tier platform that runs on WebLogic. This Fusion Middleware architecture enables fast performance, optimized memory usage, high concurrency, flexible deployment options, and failover. Essbase utilizes Oracle Database and/or your choice of supported relational database to store Essbase schemas.

Security — In Essbase On-Premise installations, all data can be encrypted in transit layer using Transport Layer Security (TLS). For user authentication, you can choose WebLogic Embedded LDAP in conjunction with your choice of external authentication provider, or if you use EPM Shared Services security, you can continue to use it.

Connectivity — With Essbase APIs, you can use TLS for secure connectivity both internally between components and externally with other applications. You can connect from any software using Essbase Runtime Client (RTC) over secure HTTP without needing to open additional TCP/IP ports to enable client connectivity.

Failover — In Essbase 11g On-Premise, Provider Services enabled failover leasing managed through OPMN. Now, failover is integrated with WebLogic to support a central request leasing system that determines which node is active and which are on standby.

Configuration — Most configuration parameters you need for application tuning should be set per application. You also have control of the system-wide configuration defaults in authentication file, if needed.

Essbase Administration Services Lite — Although Essbase has a modern administration interface and platform features, you can use Essbase Administration Services (EAS) lite as an option for continued management of your applications. It offers the same EAS functionality that you had in Essbase 11g, and is available for a limited time, to assist with your adoption of the new administration interface.

Logging — Logs are in Oracle Diagnostic Logging (ODL) format. You can download log files from Essbase, and use Performance Analyzer to analyze Essbase logs to generate usage and performance statistics.

# Differences Between Essbase Deployment Options

Review this topic to learn the differences between Essbase 21c deployment options.

For an Essbase 21c independent deployment, you install and configure Essbase using installation and configuration tools available on Oracle Software Delivery Cloud.

If you select to use Essbase 21c deployment on Oracle Cloud Infrastructure, you do not need to run the installation and configuration tools. The deployment process sets up Essbase on your Oracle Cloud Infrastructure (OCI) tenancy. Access the deployment stack listings from Oracle Cloud Marketplace.

| Feature or Component | Independent Deployment | Stack Deployment on OCI |
|---|---|---|
| Integration with EPM System Foundation Services | Yes | No |
| Built-in integration with Identity Cloud Service | No | Yes |
| Support for failover configuration | Yes | No |
| Essbase Administration Services (EAS Lite) | Yes | No |
| Support for federated partitions to Autonomous Data Warehouse | No | Yes |
| Support on Windows | Yes | No |
| Support for centralized Smart View URL for multiple Essbase instances | Yes | No |
| Support for Smart View for Office (Mac and Browser). | No | Yes |
| Encrypted applications | No | Yes |

# Differences Between Essbase 11g and Oracle Essbase 21c

To understand the latest Oracle Essbase platform, review these differences in features and functionality from Essbase 11g On-Premise to Oracle Essbase 21c.

For differences in Essbase deployment types, see Differences Between Essbase Deployment Options.

**Architecture/Core Engine**

| Feature or Component | Essbase 11g | Essbase 21c | Notes |
|---|---|---|---|
| Application Architecture | EPM System, Foundation Services | Essbase runs on a middle-tier WebLogic platform, either in Fusion Middleware or Oracle Cloud Infrastructure. | In independent deployments, Fusion Middleware enables fast performance, optimized memory usage, high concurrency, flexible deployment, and failover.<br>In deployments on Oracle Cloud Infrastructure, you do not have to run Essbase install/configuration tools. OCI enables fast performance, optimized memory usage, and flexible deployment. |

| Feature or Component | Essbase 11g | Essbase 21c | Notes |
|---|---|---|---|
| Relational Database for Essbase metadata | No | Yes | Repository Creation Utility (RCU) schemas hold information about Essbase platform artifacts and components. This metadata is stored in a supported relational database (RDBMS) of your choosing. Note that your Essbase applications and cubes aren't stored in these schemas. For independent deployments, applications are in your selected <Application Directory> location on the server where you install Essbase. For deployments on Oracle Cloud Infrastructure, applications are in the data block volume on your Essbase compute instance. |
| Query Engine Options (aggregate storage, block storage, hybrid mode) | Block storage default | Hybrid mode default | Hybrid mode is the default for block storage cubes, providing robust dependency analysis, fast aggregation, ability to process more calculations, and several tuning options. See Adopt Hybrid Mode for Fast Analytic Processing. |
| Failover | Yes | Yes (independent deployment on Linux only) | Failover is integrated with WebLogic to support a central request leasing system that determines which node is active and which nodes are waiting on standby. |
| Unicode | Yes | Yes | Essbase 21c uses UTF-8 encoding. Convert all native-encoded Essbase 11g On-Premise applications to Unicode before running the LCM export operation. |

### Interfaces/Tools

| Feature or Component | Essbase 11g | Essbase 21c | Notes |
|---|---|---|---|
| Administrative Essbase Web Interface | No | Yes | The Essbase web interface enables you to manage applications, users/groups, and Essbase artifacts. It includes a rich outline editor, scripting editors, a data analysis interface where you can save grid layouts, and a load rules editor with built-in data previews. A centralized Jobs interface lets you initiate requests, and monitor active and recent requests. Cube Designer and Smart View, as well as utilities for migration, automation, and administration, are available to download from the Console. |
| Cube Designer, Application Workbooks | No | Yes | The Cube Designer extension for Microsoft Excel is a client interface for designing and building Essbase cubes from application workbooks. This interface offers a flexible and portable cube design and administration system. Structured workbooks simplify everyday cube design, optimization, and portability. Cube Designer infers patterns found in unstructured workbooks, to help you shape raw data into hierarchically organized cubes. Cube Designer and application workbooks also offer the benefit of offline cube development and the ease of iterative builds. See Work with Cubes in Cube Designer. |
| Migration, Backup/Restore | Yes | Yes | Essbase makes it convenient to migrate applications across Essbase releases and host servers, using a choice of utilities via the Console, depending on the migration path; see About Migration Tools and Uses Cases. You must also maintain regular backups of the Essbase RCU schemas stored in a relational database, as well as user roles. Consult the back up and restore instructions for your deployment type. |
| Catalog | No | Yes | The Catalog is a central place to store files and artifacts associated with Essbase applications and users. It includes user and shared directories, and an instructive Gallery of sample cubes. |

| Feature or Component | Essbase 11g | Essbase 21c | Notes |
|---|---|---|---|
| Gallery | No | Yes | Included in the Catalog is a Gallery of cube templates, in the form of Excel application workbooks. Import these workbooks to build a diverse variety of sample cubes. The samples are instructional for learning about different use cases for Essbase applications and features, as well as learning how to build and design cubes from structured and unstructured workbooks. |
| Smart View | Yes | Yes | See Working with Oracle Smart View for Office. |
| Provider Services | Yes | Yes | Provider Services is built in to Essbase 21c. Provider Services requests time out by default after 10 minutes. Configuration options are available in the Console. You must update client service URLs to the new format, as described in migration instructions. |
| Essbase Administration Services | Yes | Yes (Independent deployment only) | EAS Lite is an option (with independent deployment) for continued management of your applications, in case your company is not ready to adopt the web interface. The features and functionality of EAS are limited to what was available in Release 11g and do not encompass the modern platform features. |
| Essbase Studio | Yes | No | Use connections and Datasources to connect to your outside sources of data, use the improved Rules editor to preview and shape imports to your cube, and use Drill Through reports to access data you won't import. |

### Security/Authentication

| Feature or Component | Essbase 11g | Essbase 21c | Notes |
|---|---|---|---|
| Communication/ Network Security | Security file | TLS, load balancer | All data is encrypted in transit layer using Transport Layer Security (TLS). You can optionally implement a load balancer. On independent deployments, this could be Oracle HTTP Server or another load balancer you choose. On Oracle Cloud Infrastructure deployments, you can select to configure a load balancer through OCI. |
| Authentication Method | EPM Shared Services or native | Oracle Identity Cloud Service (OCI deployment only)<br>EPM Shared Services (independent deployment only)<br>WebLogic Embedded LDAP | On independent deployments, for user and group authentication, choose WebLogic Embedded LDAP, or if you already use EPM Shared Services, you can continue to use it with Essbase 21c (independent deployment). If you select WebLogic, it is strongly recommended to federate users to an external authentication provider, such as Microsoft Active Directory, which is suitable for production environments.<br>On OCI deployments, (including when using MSAD) integrate with Oracle Identity Cloud Service (IDCS). |
| User/Group Roles and Application Permissions | Essbase roles, Shared Services roles, and application roles | Simplified: 3 roles, 4 permissions | Essbase user roles are User, Power User, and Service Administrator. Application permissions, granted separately, are Application Manager, Database Manager, Database Update, and Database Access. All roles from EPM Shared Services can be mapped to the new roles and permissions, or, you can continue to use EPM Shared Services (independent deployment only). |

| Feature or Component | Essbase 11g | Essbase 21c | Notes |
|---|---|---|---|
| Filters | Yes | Yes | Filters help you implement fine-tuned, cell-level access controls to your cubes. Using dynamic filters with built in functions/variables, you can make filters extensible and adaptable to a changing user base and real-time source data. You can use LoginAs to test the filters in the Essbase web interface.<br>In Essbase 11g On-Premise, only one filter can be granted per user per cube. In Essbase 21c, new filter assignments are combined with existing filter assignments. |
| Security file | Yes | No | There is no need for essbase.sec in Essbase 21c. |

### Data Connectivity/Interoperability

| Feature or Component | Essbase 11g | Essbase 21c | Notes |
|---|---|---|---|
| Connections and Datasources | No | Yes | Essbase administration tasks often require connectivity to remote source data or hosts. With reusable connections and Datasources, you no longer have to code the connection details into artifacts like rule files or filters, or enter them each time you perform other connection-dependent tasks. |
| Network Connectivity | Yes | Yes | Essbase APIs use TLS/SSL for secure connectivity both internally between components and externally with other applications. You can connect from any software using Essbase Runtime Client (RTC) over secure HTTP without needing to open additional TCP/IP ports to enable client connectivity. |
| Partitions | Yes | Yes | Linked partitions aren't supported in Essbase 21c. Use @XREF and @XWRITE to analyze data across cubes. See Link Cubes Using Partitions and XREF/XWRITE.<br>The administrator must set up user security for the source and target cubes. See Security for Partitioned Databases.<br>For OCI deployments, federated partitions are available with Autonomous Data Warehouse, enabling transparent integration of relational data and the Essbase cube. |
| Drill Through | Yes | Yes | When you need more data than what is in the cube, use Drill Through reports to access external data sources. Performance is improved for drill through connections to Oracle Database. The flexibility of Drill Through report design is improved, allowing diversified selection of multiple cells or ranges of cells. Selections can be recursive, non-recursive, level 0, contiguous, or non-contiguous. |

### Calculation/Data Flow

| Feature or Component | Essbase 11g | Essbase 21c | Notes |
|---|---|---|---|
| Calculation Scripts (block storage and hybrid mode) | Yes | Yes | Full library of calculation functions and commands suits most analytical applications. Build your own custom defined functions and macros. Calculation tracing helps analyze and debug calc script performance and member formula processing. Tuple-based calculation helps optimize and refine calculation scope, limiting it to focus on the active Smart View grid. Hybrid calculation can be used, and offers tuning options. |
| Aggregate Storage Calculation | Yes | Yes | MDX Insert helps you perform custom calculations and allocations. You can automate the creation and maintenance of default aggregate views. |

| Feature or Component | Essbase 11g | Essbase 21c | Notes |
|---|---|---|---|
| Hybrid query processor enabled by default for block storage cubes | No | Yes | Essbase 21c processes dynamic dependencies in queries using hybrid mode. In hybrid mode, Essbase evaluates formula dependencies prior to resolving queries, ensuring minimal processing time and accurate results.<br>Hybrid mode is not the default mode for calculation scripts, but you can enable it using the HYBRIDBSOINCALCSCRIPT configuration setting.<br>In Essbase 11g, the default query engine is not hybrid mode, but you can enable it using ASODYNAMICAGGINBSO.<br>**Note:**<br>Do not use two-pass calculation with hybrid mode cubes. Only use solve order. |
| Parallel Calculation | Yes | Yes | See Using Parallel Calculation. |
| Data Load/Dimension Build Rules | Yes | Yes | Load rules editor has built-in data previews. You can import from the Catalog or from outside sources. Rule file columns can employ functions like Sum, Min, Max, Count, and Avg, to help you shape your import. Performance is improved for SQL-based loading. Batch Outline Editing is available from Java or REST API. Command-line interface (CLI) supports streaming data load from a variety of sources. Aggregate storage data load optimizations include buffer, merge, and cache tuning options. You can migrate rule files from Essbase Studio and edit them in the Essbase web interface. |
| Custom-Defined Calculation Functions and Macros | Yes | Yes | Build your own custom-defined functions and macros in Java. |
| MDX | Yes | Yes | In addition to MDX's well-known utility as a multidimensional query language, you can use its Insert and Export directives to shape, copy, move, and update any custom slice of multidimensional data. Sub Select lets you filter the volume of queried data. |
| Two pass calc | Yes | Not recommended | Do not use two-pass calculation with hybrid mode cubes. Only use solve order. |
| Scenario Management | No | Yes | Scenario management offers the ability to build private work areas or "sandboxes" in which users can model different assumptions within the data to see the effect on aggregated results, without affecting the cube. |

### Development, Automation, and Audit

| Feature or Component | Essbase 11g | Essbase 21c | Notes |
|---|---|---|---|
| Automation and Developer Tools | Yes | Yes | REST API helps you automate management of Essbase resources over secured HTTP. Java API, Command Line Interface (CLI), MaxL administrative language, and Report Writer are also available. |
| Accelerated Development and Audit Capabilities | No | Yes | Calculation tracing lets you monitor and debug calculation scripts. Query tracing can be used to monitor and debug query performance. Audit trail enables you to track changes made to data. Solve order can be adjusted while you're working in Smart View. |

| Feature or Component | Essbase 11g | Essbase 21c | Notes |
|---|---|---|---|
| Shadow Applications | No | Yes | To perform cube modifications and restructures with limited down time, you can create a shadow application that is a copy of the primary application. The primary application continues to serve read-only operations, such as queries, while you perform modifications on the shadow application. You can make the shadow application visible or hidden. Available in REST API – see the Create Shadow Application endpoint. |

### Configuration

| Feature or Component | Essbase 11g | Essbase 21c | Notes |
|---|---|---|---|
| Configuration Tool | No | Yes (independent deployment only) | For independent deployments, you can configure your Essbase environment any time using the integrated configuration tool, either at the end of your Essbase installation, or by launching the Configuration Tool later, after installation. Silent mode is available if you're configuring frequently (for example, in a development environment). |
| Configuration Settings | Yes | Yes | Most configuration parameters you need for application tuning should be set per application, using the Essbase web interface. Server-level configuration is handled by the configuration tool (for independent deployments), but you can also change server configuration defaults using essbase.cfg, if needed. Provider Services configuration options for network-related preferences are available in the Console. |

### Other Notable and Legacy Features

| Feature or Component | Essbase 11g | Essbase 21c | Notes |
|---|---|---|---|
| Expanded Analysis Methods | No | Yes | You can perform ad hoc data queries/grid analyses on cube data from the administrative Essbase web interface, as a built-in alternative to connecting via Smart View. You can save your grid layouts, run report scripts, and run and save named MDX queries. See Analyze Data in the Web Interface. |
| Member ID | No | Yes | A unique Member ID is automatically assigned to every member in the cube outline. |
| Logging | Yes | Yes | Application logs are in Oracle Diagnostic Logging (ODL) format. You can download them from the Essbase web interface. You can use Performance Analyzer to analyze Essbase logs to generate usage and performance statistics. |
| Implied Sharing | True by default | You choose | In Essbase 11g On-Premise, the implied share setting could be changed for an application using the IMPLIED_SHARE setting. When you migrate an Essbase 11g On-Premise application to Essbase 21c, your IMPLIED_SHARE setting is preserved. For each application, you set implied share behavior only once, at application creation time (it's not meant to be changed). See IMPLIED_SHARE_ON_CREATE configuration property, which is FALSE by default (unless you migrate an application that has IMPLIED_SHARE set to TRUE). |
| Report Scripts | Yes | Yes | See Report on Data. |
| Currency Conversion | Yes | Yes | See Designing and Building Currency Conversion Applications. |
| ESSCMD | Yes | Yes | ESSCMD is still supported, but is not updated with the latest features. Try CLI and MaxL. |

| Feature or Component | Essbase 11g | Essbase 21c | Notes |
|---|---|---|---|
| Varying Attributes | Yes | Only in EAS Lite (for independent deployments) | - |
| Hybrid Analysis | Yes | No | Not applicable in Essbase 21c. Use connections and Datasources to connect to your outside sources of data, use the improved Rules editor to preview and shape imports to your cube, and use Drill Through reports to access data you won't import. |
| Incremental Restructuring | Yes | No | Restructuring is not as time-consuming in Essbase 21c. If needed, you can work in a shadow application to limit down-time. |
| Dynamic Calc and Store | Yes | No | Dynamic Calc and Store members are treated as Dynamic Calc. |
| Direct I/O, cache memory locking | Yes | No | Not applicable |
| Disk volumes | Yes | Yes | Set up disk volumes using standard operating system mounts, instead of DISKVOLUMES configuration property. |
| Repair Invalid Block Headers | Yes | No | Not applicable |
| Data Compression Types: Zlib, None | Yes | No | Not applicable |
| Isolation modes | Yes | No | Essbase 21c manages block storage data transactions in uncommitted mode. Essbase releases a block after it is updated, and commits blocks when the transaction is completed. |

# Typical Workflow for Administrators

Use this workflow as a high-level guide to administrator tasks for installing and maintaining Essbase.

| Task | Description | More Information |
|---|---|---|
| Before You Begin | Review and address the prerequisites, flow, and some considerations before installation and configuration | Before You Begin |
| Install Essbase | Enter field values and select options for installing Essbase. | Install Oracle Essbase |
| Configure Essbase | Enter values and select options for configuration. | Configure Oracle Essbase |
| Manage security for system and network communication | Read an overview of options and related tasks. | Select Identity Provider<br>Secure Your Communication and Network |
| Migrate existing Essbase applications, users, data, and content | Migrate applications and data from Essbase 11g On-Premise. | Migrate Essbase Applications |
| Manage user roles and permissions | Set up roles for your users and assign appropriate privileges. | Manage Essbase User Roles and Application Permissions |

| Task | Description | More Information |
| --- | --- | --- |
| Manage and maintain Essbase server operation | Manage the operation of Essbase, including start/stop servers, backup/restore, patching, unconfigure, uninstall, and more. | Manage Server Operations |

2

# Before You Begin

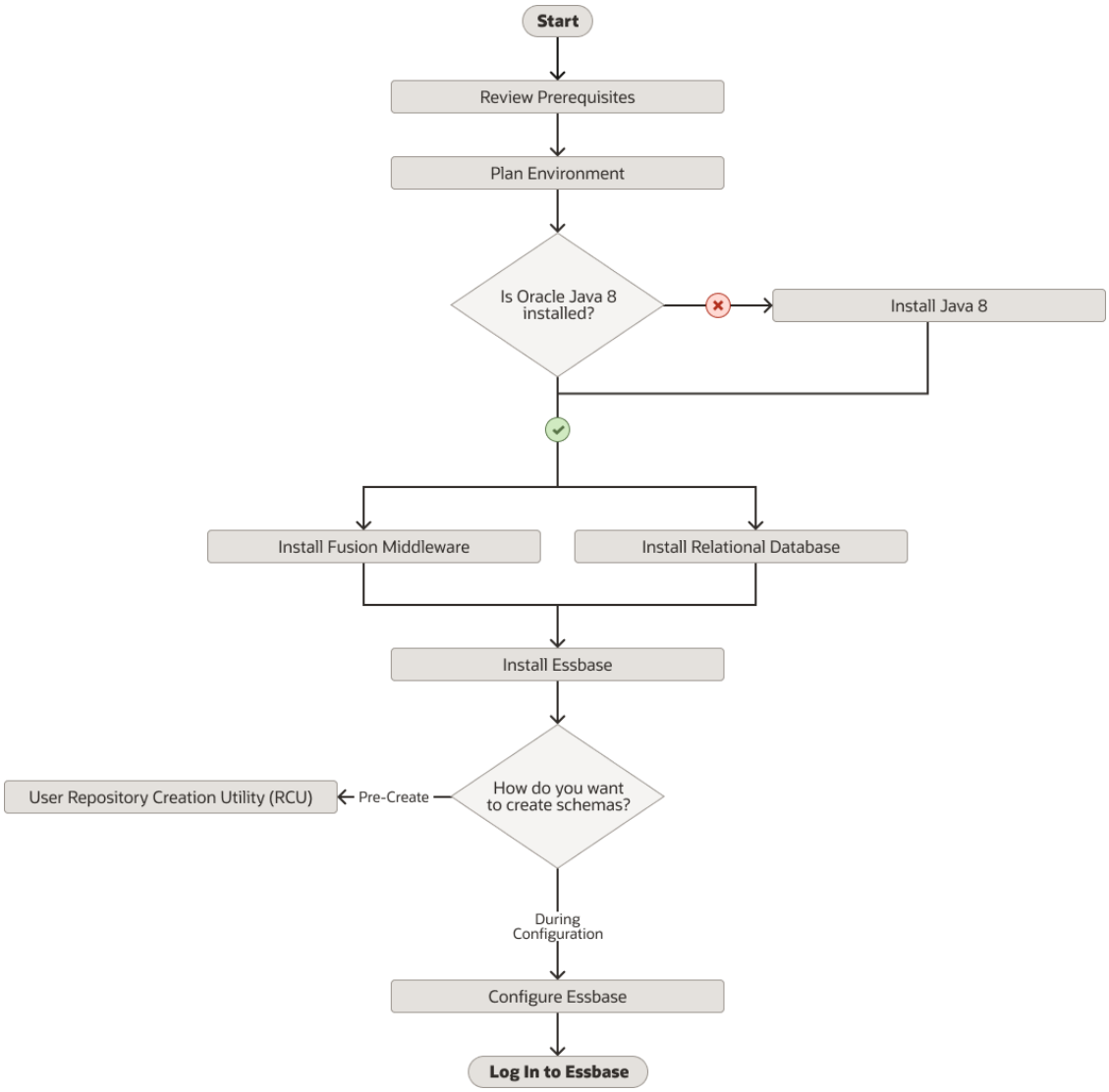
Let's explore what you need to know and do to run installation and configuration.

**Topics**



## Installation and Configuration Workflow

The following is the workflow for installing and configuring.




**Related Resources**

- Prerequisites and Considerations

- Plan Environment
- Install Fusion Middleware
- Install a Relational Database
- Install Oracle Essbase
- Pre-create RCU Schemas for Essbase
- Configure Oracle Essbase

# Prerequisites and Considerations

Before you begin to set up Oracle Essbase, here are prerequisites and considerations that you must review and address.

**Oracle Fusion Middleware Infrastructure-specific requirements**
If Oracle Fusion Middleware Infrastructure isn't already installed, you must install it before installing Essbase. See Install Fusion Middleware for installation prerequisites and instructions.

**Essbase-specific requirements and considerations**

1. In addition to those listed below, see the deployment-specific prerequisites in Install Essbase on Linux or Install Essbase on Windows .
2. For currently supported software versions, see Oracle Certification Matrix. For example, use the supported version of Oracle Database and Microsoft SQL Server as shown in Certification Matrix. You must have sysdba (or admin) user access to a supported relational database that is network-accessible to your Essbase instance. For best performance, the database should be in the same physical location (data center). See Install a Relational Database, and use the documentation for your selected RDBMS.
3. For platform environment considerations: See Plan your platform environment.
4. Ensure that the ephemeral port range used by the operating system doesn't conflict with any reserved Essbase ports. See Avoid Port Conflicts.
5. Before using the current Essbase product version, apply the certified patches listed in the relevant topic in the Oracle Essbase Release Notes.
6. For customers who use Teradata: to make connection to the Teradata database, the host that runs Essbase must have Teradata client drivers installed.

## Plan Your Essbase Environment

Oracle recommends you use separate disk volumes or directories for the software binaries, Essbase application data, and WebLogic domain configuration. You provide these locations in the installation and configuration procedures.

Fusion Middleware and a relational database are prerequisites to installing Essbase.

### About the Relational Database

Before you can configure Essbase, you need network connectivity to a relational database where the Essbase and Fusion Middleware RCU schemas reside.

Oracle recommends deploying a distinct pluggable database (PDB) for Essbase. You can read about Oracle's multitenant architecture here: Introduction to Multitenant Architecture.

- No other applications should have access to the Essbase repository schemas generated by the Repository Creation Utility (RCU).

- No one else other than the designated administrator should have permission to access the schemas or their tables.
- No one else should have the credentials to assign or change roles to access the PDB.
- Every change to the PDB should be logged.

**About Essbase <Oracle Home>**

Install Essbase to the same <Oracle Home> as Fusion Middleware.

**Using Mounted Volumes**

For portability, it's optimal to mount a separate disk volume (networked drive) at the system root, and use it for the <Application Directory> and <Domain Root>/<Domain Name> directories.

WebLogic domains and Essbase applications require a path on disk. You define these locations during the Essbase configuration. Oracle recommends that you keep Essbase <Application Directory>, <Domain Root> directories, and <Oracle Home> separate.

**About the <Domain Root>**

The <Domain Root> is the path into which WebLogic domains are created on your system. If you don't pre-create a directory for <Domain Root>, the configuration tool creates it for you based on the path you specify. Allow at least 1.5G of disk space.

**About the <Application Directory>**

The <Application Directory> you select is where Essbase stores your application data (block, page, and index files). If you don't pre-create one, the configuration tool creates it for you based on the path you specify for <Application Directory>. Select a location separate from the location of software binaries. Allow enough disk space for your applications; Oracle recommends 1T.

**See Also**

Environment Locations in the Essbase Platform

# Install a Relational Database

Before you can configure Essbase, you need network connectivity to a relational database with target Essbase Repository Creation Utility (RCU) schemas.

For information about Repository Creation Utility, see Pre-create RCU Schemas for Essbase.

For instructions, see the documentation for the supported relational database that you select. For Oracle Database 21, see Database Installation Guide for Linux.

# Install Fusion Middleware

Essbase requires Fusion Middleware as a middle-tier platform. If it's not already installed, install Fusion Middleware or the latest patch, into your Oracle Home directory before you install Essbase.

**Prerequisites**

- For **Linux** deployments: Linux Operating System Requirements for Fusion Middleware

- For **Windows** deployments: Windows Operating System Requirements for Fusion Middleware
- GCC-(Database client GNU Compiler Collection), a C compiler, must be installed.
- JDK Requirements
- General Memory and Disk Space Requirements and Oracle Fusion Middleware Infrastructure Disk Space Requirements
- Network Requirements
- Database Requirements
- For additional reference, see Installing and Configuring the Oracle Fusion Middleware Infrastructure.

**To install Fusion Middleware:**

1. If you haven't already, download Oracle Fusion Middleware 12c Infrastructure 12.2.1.4.0.
2. Run the Fusion Middleware installation jar file.

   ```
   $ java -jar fmw_12.2.1.4.0_infrastructure.jar
   ```

   The installer software is extracted. If it doesn't extract, ensure that you're using Oracle Java 8.

   If requested or you want to specify:

   - For the Inventory Directory, specify a central inventory directory for all Oracle installations. For example, `/scratch/user/oracle_home/user_projects/oraInventory`.
   - For the Operating System Group, select your group, and click **OK**. The default value is dba.
3. On the Welcome page, click **Next**.
4. Select your choice to skip automatic updates, select patches, or search My Oracle Support for the latest software updates, and click **Next**.
5. For installation location, specify your **Oracle Home** directory. For example, `/scratch/user/oracle_home`. This Oracle Home directory should be empty. Click **Next**.
6. For installation type, select your option of Fusion Middleware Infrastructure and click **Next**.
7. The installer will check for Java version and operating system. Review the prerequisite checks and click **Next**.
8. Review the installation summary. Note down the log file location of Fusion Middleware install logs, if needed. Alternatively you can choose to click **Save Response File** in order to use it later during the silent mode installer.
9. Click **Install**.

   After the installation completes, click **Finish** to exit the installer.

3

# Install Oracle Essbase

Learn about installing using the Essbase Installer or Silent Mode.

**Topics:**



## Install Essbase on Linux

You're ready to install Essbase on Linux, once the prerequisites are reviewed and addressed.

**Prerequisites and Notes**
Before you install, review the prerequisites and notes listed below, and also those listed in Prerequisites and Considerations.

- Supported version of Oracle Fusion Middleware Infrastructure must be installed. See prerequisites for Install Fusion Middleware.Supported version of Linux server must be used for the installation.
- GCC-C++ (Database client GNU Compiler Collection), a C compiler, must be installed on the Linux machine.
- If you're using the Essbase interface (UI)-based Installer or Configuration Tool, a graphical X Linux interface, such as Xterm, is required.
- For Oracle Essbase, the latest version of Oracle JDK 8 must be installed. See Fusion Middleware Oracle Java Requirements. Because Essbase requires Fusion Middleware as a prerequisite, Essbase strictly adheres to the Java minimum requirements used by Fusion Middleware. Java 8 must be in the PATH environment variable of the user performing the installation.
- When Essbase is installed, you receive access to the required services based on your defined role and permissions.
- There are optional arguments you can enter on the command line, when you launch installation. See Installer Options - Syntax and Commands.

**Run Essbase Installer**

1. If you haven't already, download the installer software for Essbase 21c.
2. Run the Essbase installation jar file.

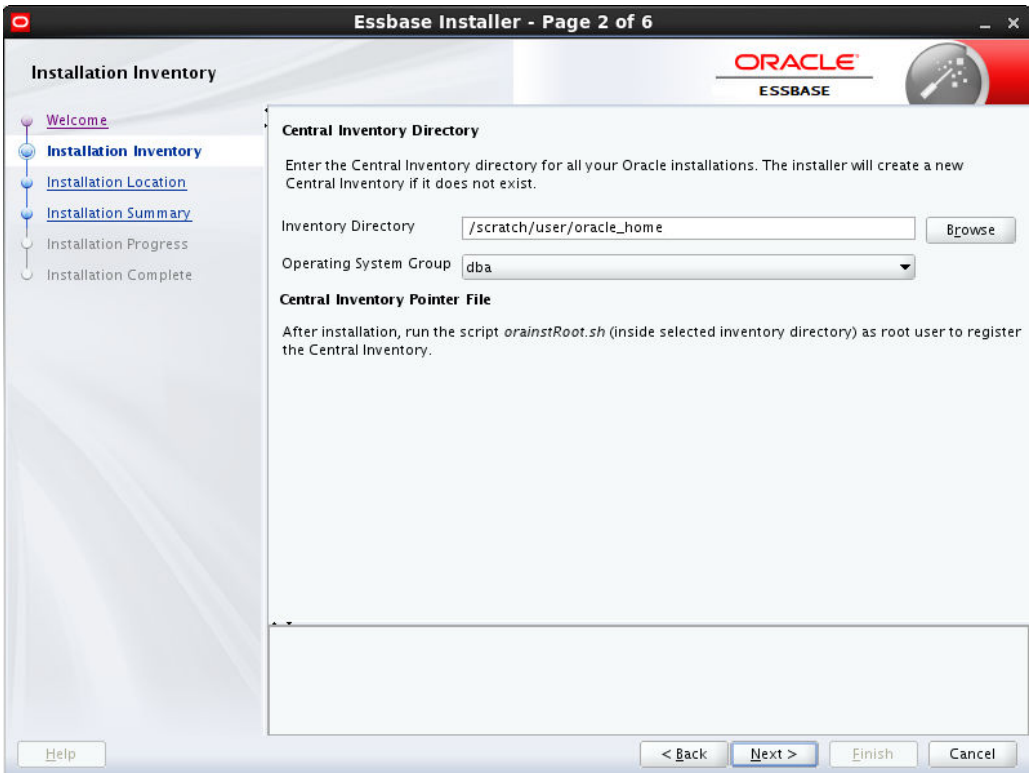
   For example:

   ```
   $ java -jar essbase-21.1.x.x.x-nnn-linux64.jar
   ```

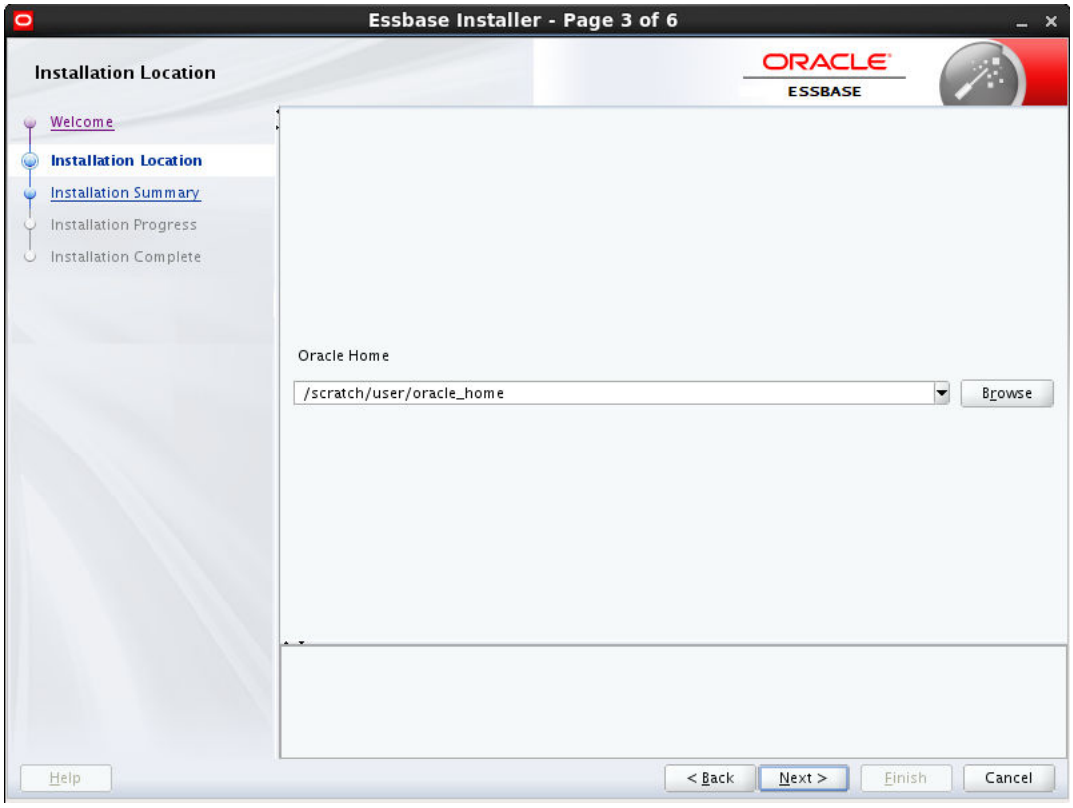
   The inventory location parameter `-invPtrLoc <file>` can be added, and the <file> value entered with the full path and name of the `oraInst.loc` file; this can be found in the Oracle Home folder where Fusion Middleware is installed. See Specify Inventory Location.

When you enter the above java command, the installer software is extracted. If it doesn't extract, ensure that you're using Oracle Java 8.

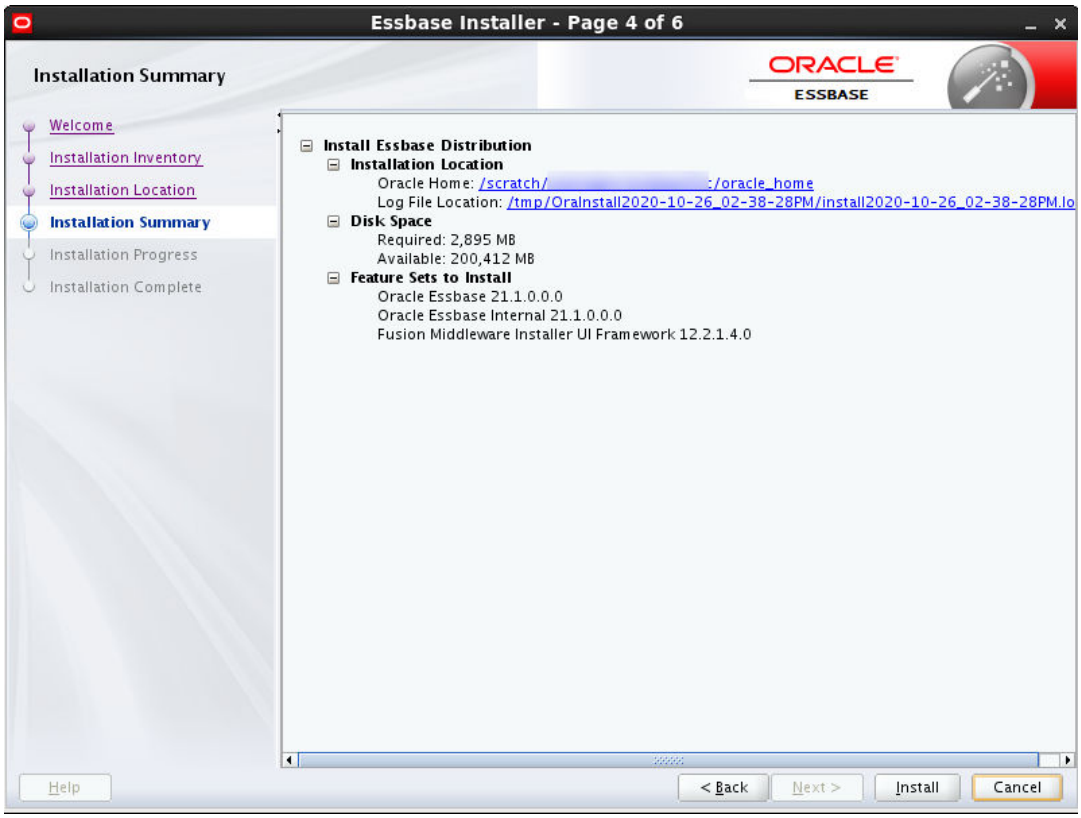
3. Review the Welcome page and click **Next**.
4. If the Installation Inventory page is displayed, as shown in the following window example, do the following steps.
   a. For Inventory Directory, select the same one used by Fusion Middleware, such as *<Oracle Home>*.



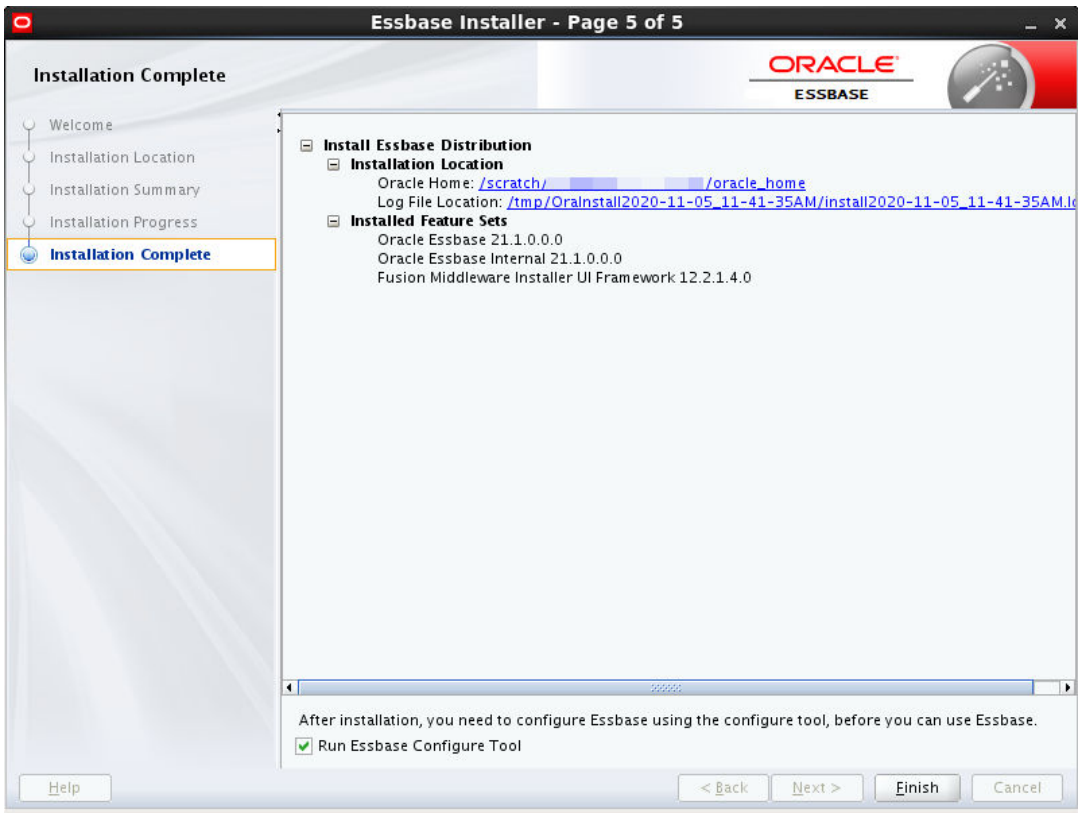

   b. For Operating System Group, your primary operating system group for your username is detected (for example, dba). Accept the default and click **Next**. If you encounter an inventory location error, see Specify Inventory Location.
5. For Installation Location, enter the same <Oracle Home> directory that you used for Fusion Middleware (for example, `/scratch/user/oracle_home`). Click **Next**.




6. Review Installation Summary (an example is shown below), and click **Install**.



7. You can monitor the status on the Installation Progress page. After it reaches 100%, click **Next**.
8. The Installation Complete page is displayed.




   a. If you want to proceed now with configuration, select the **Run Essbase Configure Tool** check box. To complete configuration later (for example, if you choose to pre-create RCU schemas now), leave the check box unselected.
   b. Click **Finish**.

# Install Essbase on Windows

You're ready to install Essbase on Windows, once the prerequisites are reviewed and addressed.

**Prerequisites and Notes**
Before you install, review the prerequisites and notes listed below, and also those listed in Prerequisites and Considerations.

- Supported version of Windows - 2019 or above.
- Supported version of Oracle Java SDK - latest build of JDK 1.8 must be pre-installed.
- SET JAVA_HOME as env variable.
- Supported version of Oracle Fusion Middleware Infrastructure must be installed. See prerequisites and instructions in: Install Fusion Middleware.
- When Essbase is installed, you receive access to the required services based on your defined role and permissions.

- There are optional arguments you can enter on the command line, when you launch installation. See Installer Options - Syntax and Commands.

**Run Essbase Installer**

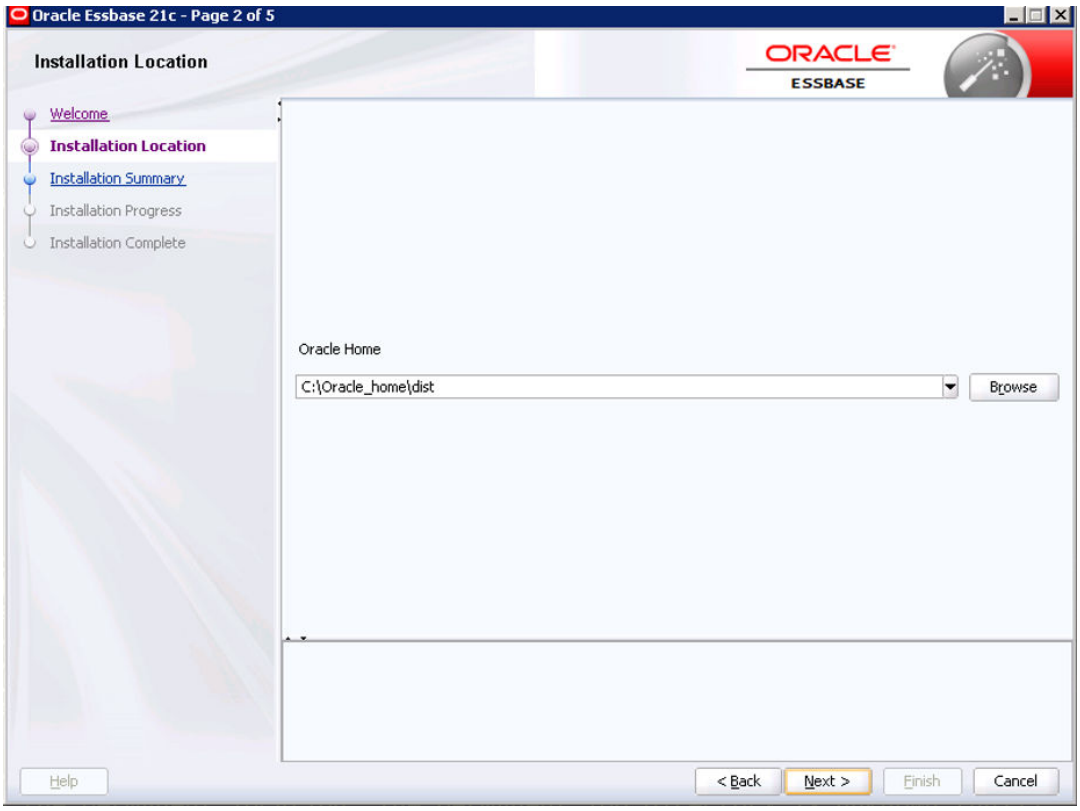
1. If you haven't already, download the installer software for Essbase 21c from https://edelivery.oracle.com/osdc/faces/Home.jspx.
2. Run the Essbase installation jar file.

   For example:

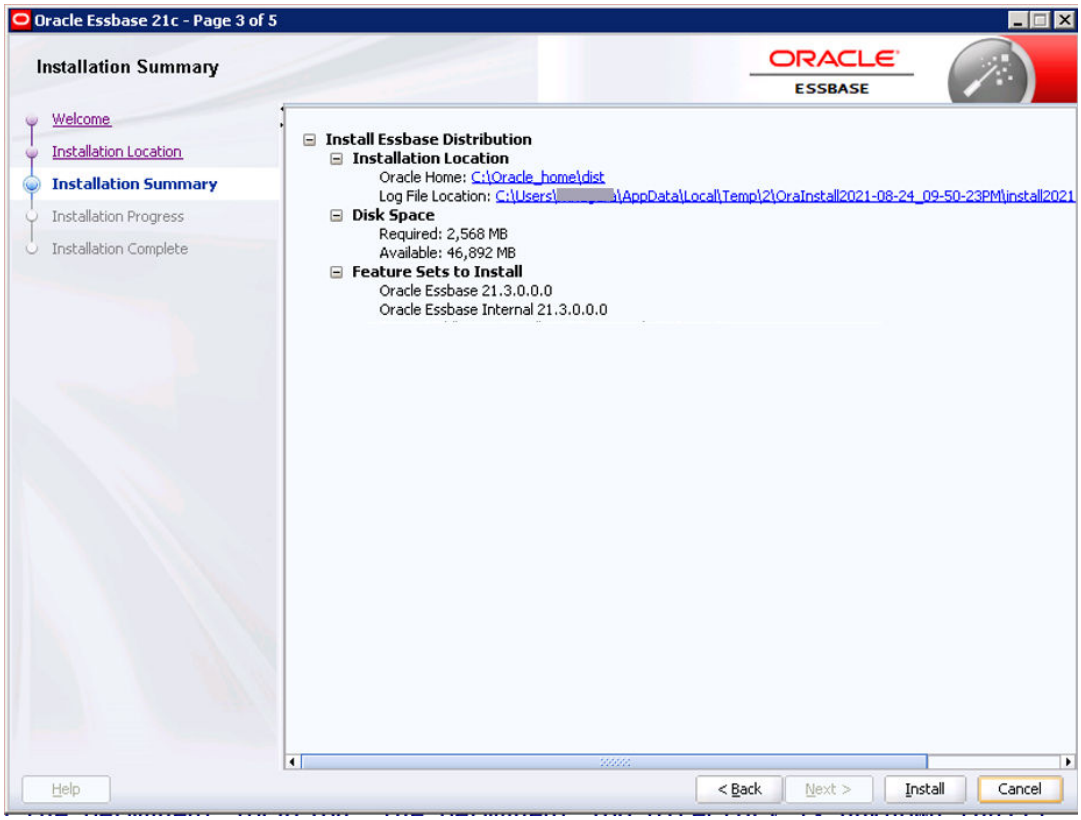
   ```
   C:\Program Files\Java\jdk1.8.0_xxx\bin\java.exe -jar
         essbase-21.x.x.x.x-nnn-win64.jar
   ```

   The inventory location parameter `-invPtrLoc <file>` can be added, and the <file> value entered with the full path and name of the `oraInst.loc` file; this can be found in the Oracle Home folder where Fusion Middleware is installed. See Specify Inventory Location.

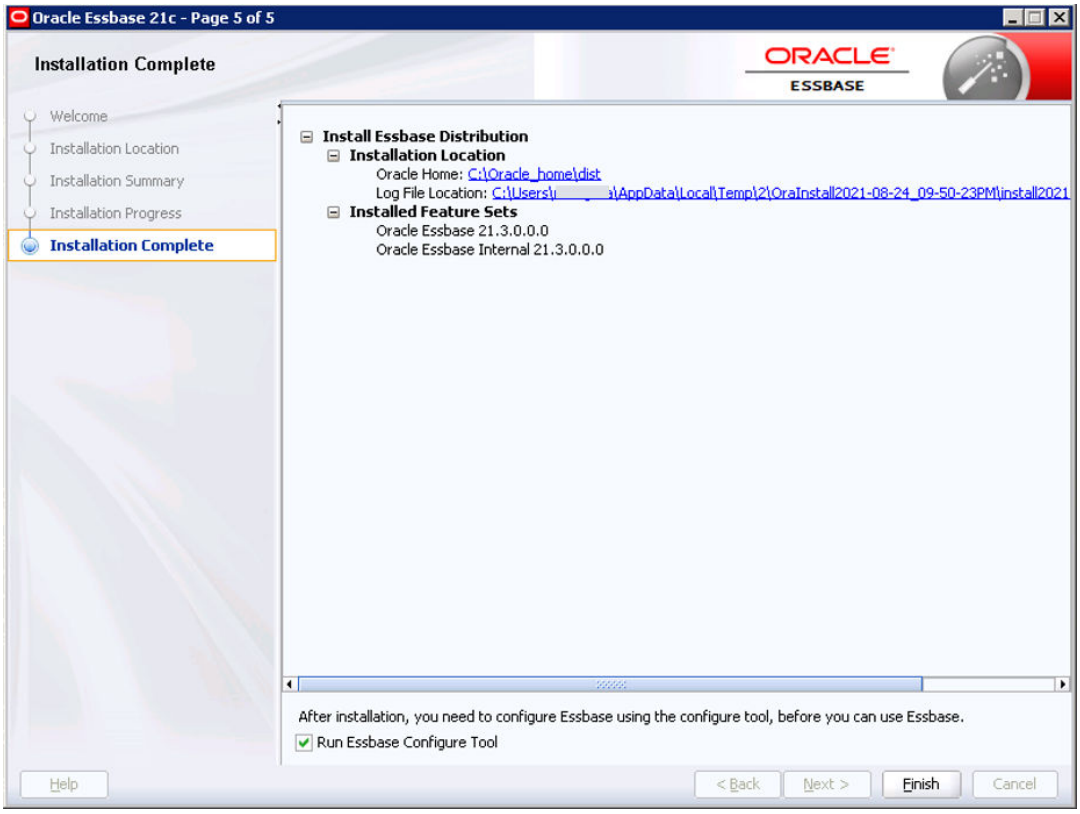
   When you enter the above java command, the installer software is extracted. If it doesn't extract, ensure that you're using Oracle Java 8.
3. The Next Generation Oracle Universal Installer opens. Review the Welcome page and click **Next**.
4. For Installation Location, enter the same <Oracle Home> directory that you used for Fusion Middleware installation, for example, `c:\oracle_home\dist`. Click **Next**.




5. Review Installation Summary (an example is shown below), and click **Install**.




6. You can monitor the status on the Installation Progress page. After it reaches 100%, click **Finish**.
7. The Installation Complete page is displayed.




a. If you want to proceed now with configuration, select the **Run Essbase Configure Tool** check box. To complete configuration later (for example, if you choose to pre-create RCU schemas now), leave the check box unselected.

b. Click **Finish**.

# Run Essbase Installation in Silent Mode

Oracle Essbase enables you to run the installation in Silent Mode, using a response file.

**Prerequisites and Notes**

- Before you install, read the prerequisites in Prerequisites and Considerations, which are the same as for the Essbase Installer. also see the installation prerequisites in Install Essbase on Linux or Install Essbase on Windows .
- You'll be prompted for passwords, or can pass them as parameters to the script.
- The script can be run with optional parameters, such as `-invPtrLoc`. See Installer Options - Syntax and Commands.

**Run Silent Mode Installation**

1. To install, run the following command:

   For Linux:

```
java -jar essbase-<version>-linux64.jar -silent -invPtrLoc <full path of
oraInst.loc>
          -responseFile <absolute_path to install.rsp>
```

For Windows:

```
java -jar essbase-<version>-win64.jar -silent -responseFile <absolute_path
to install.rsp>
```

The optional inventory location parameter, for Linux, `-invPtrLoc <file>` can be added, and the <file> value entered with the full path and name of the `oraInst.loc` file; this can be found in the <Oracle Home> folder where Fusion Middleware is installed. See Specify Inventory Location.

2. Continue with setup by doing the necessary configuration. See Run Oracle Essbase Configuration in Silent Mode.

4

# Configure Oracle Essbase

Oracle Essbase can be configured using Essbase Configuration Tool or Silent mode.

**Topics:**



## Configure Essbase on Linux

You must configure Essbase on Linux using the Configuration Tool, either at the end of the Essbase installation, or by launching the Configuration Tool later, after installation.

**Prerequisites and Notes**

- Fusion Middleware must already be installed, and Oracle Essbase must be installed in the same Oracle Home directory. See Install Fusion Middleware.
- Supported relational database must be installed, as mentioned in the installation prerequisites. See Install a Relational Database.
- If you are using EPM Shared Services authentication, you must already have a supported version of EPM installed, with EPM users Shared Services created and configured, and Know Your Oracle Home and EPM Instance Details.
  - If using EPM Shared Services authentication, it should be running during Essbase configuration. If EPM Shared Services is not running, some port numbers must be manually configured to avoid port conflicts. When you configure Essbase, you must be cautious and aware of ports that are already in use by any EPM services on this host, and to only choose and use valid ports that are not used by a service or application on this host. You must also set these unused port numbers accordingly in the user interface or in the response file.
  - If you are using Essbase 21c versions prior to 21.2.1, use an empty EPM Foundation Services instance that is separate from your production EPM instance. EPM Server must run while you configure and run Essbase. You can connect your user management directory service to both Foundation Shared Services deployments, and must maintain application provisioning in both Shared Services instances.
  - For versions prior to Essbase 21.2.1, you needed to install a separate EPM Foundation.
  - For versions of Essbase 21.2.1 and later, install or reuse an existing EPM 11.2.x (including 11.2.x Essbase), to be configured with 21.2.x.
- If you are using Microsoft SQL Server (MSSQL) as the database for Essbase repository (RCU) schemas, you must run the process to alter database and apply the correct collate, and address schema considerations, before running the Essbase configuration tool. For

more information, see Configure Microsoft SQL Server as Repository Database for Essbase Schemas.

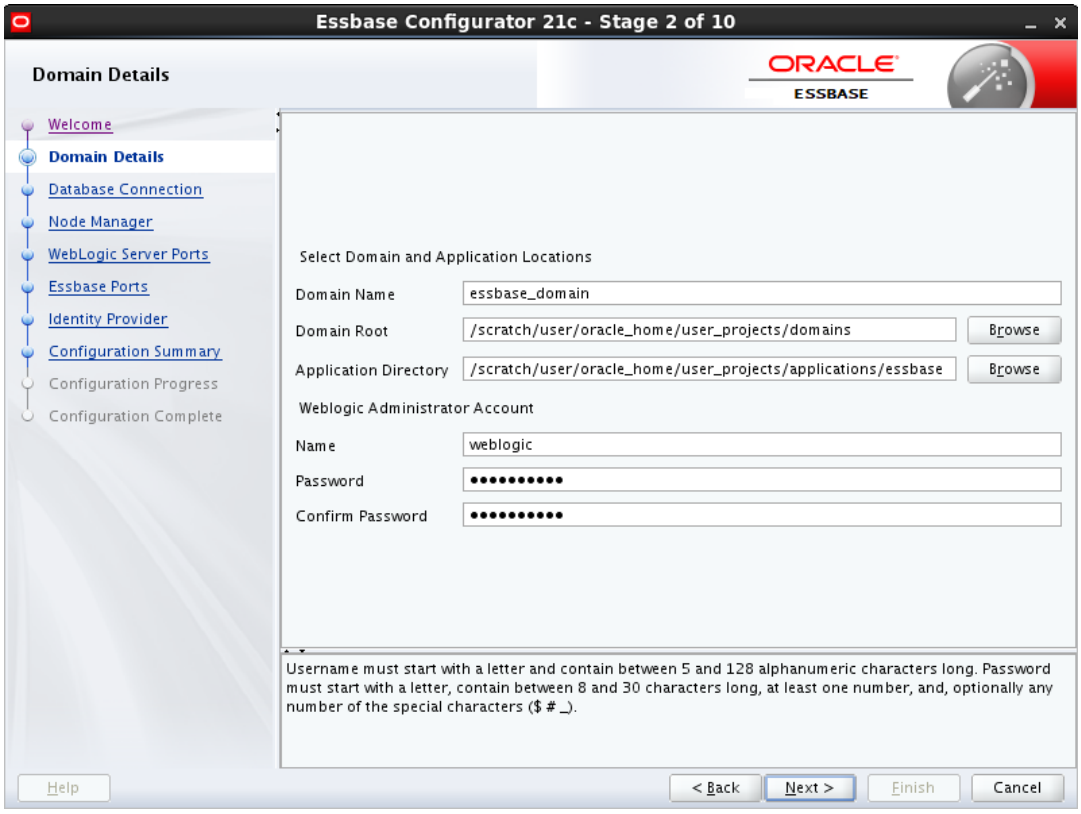
- Pre-create RCU Schemas for Essbase explains the process if you choose to pre-create RCU schemas before configuration rather then have Essbase configuration tool create them for you. One use case to pre-create schemas is if you're employing a secure HTTPS connection using a wallet.
- You must apply the following patches on Oracle Home before creating RCU schemas, whether or not you use pre-created schemas:
  - 28186730 - latest version of OPatch 13.9.4.2.x for FMW/WLS
  - 31676526 - patch 12.2.1.4.0 for TNS_ADMIN RCU warning
  - 30540494 - patch 12.2.1.4.0 for RAC RCU bug
- All ports should not be within the ephemeral ports range, nor in use by other running software. See Avoid Port Conflicts.
- Each managed server must be assigned to a machine, the logical representation of the computer that hosts one or more server instances. The machine name must be unique in relation to other configurable resources in the domain.
- If you plan to install and configure more than one Essbase On-Premise instance, to support failover, you need a front-end load balancer. See Configure a Load Balancer to Support Failover.
- If you're connecting through Smart View, using the URL `/aps/SmartView`, you need to change the URL. See Redirect to New Essbase Smart View Connection URL. Alternatively, you can configure redirection to the new URL on the web server. If you're using Oracle HTTP Server (OHS) or HTTPD Server, redirect the URL while modifying the Oracle HTTP Server configuration, as noted in the previous bullet.

### Run Configuration Tool

1. If you didn't continue with configuration at the end of installation, launch the Configuration Tool.
   a. In the Oracle Home directory, where Essbase and Fusion Middleware are installed, open a terminal in `./essbase/bin`. For example, open a terminal in `<Oracle_Home>/essbase/bin`.
   b. Launch the Configuration Tool using the config.sh script.

      ```
      $ ./config.sh
      ```

      The script can be run with parameters (such as -mode, -log, -log priority, -responseFile). If you use the responseFile parameter, all fields are filled with previous configuration entries, except for passwords. To learn about configuration script options, run: `./config.sh -help`.
2. On the Welcome page, click **Next**.
3. On the Domain Details page, do the following.




a. Accept the default (if correct) or enter your domain name, for example, `essbase_domain`

b. Accept the default (if correct) or enter your domain root path, for example,

   ```
   /scratch/user/oracle_home/user_projects/domains
   ```

   If you're installing Essbase additional instances, use a different domain root for each.

c. Accept the default or enter your application directory, for example,

   ```
   /scratch/user/oracle_home/user_projects/applications/essbase
   ```

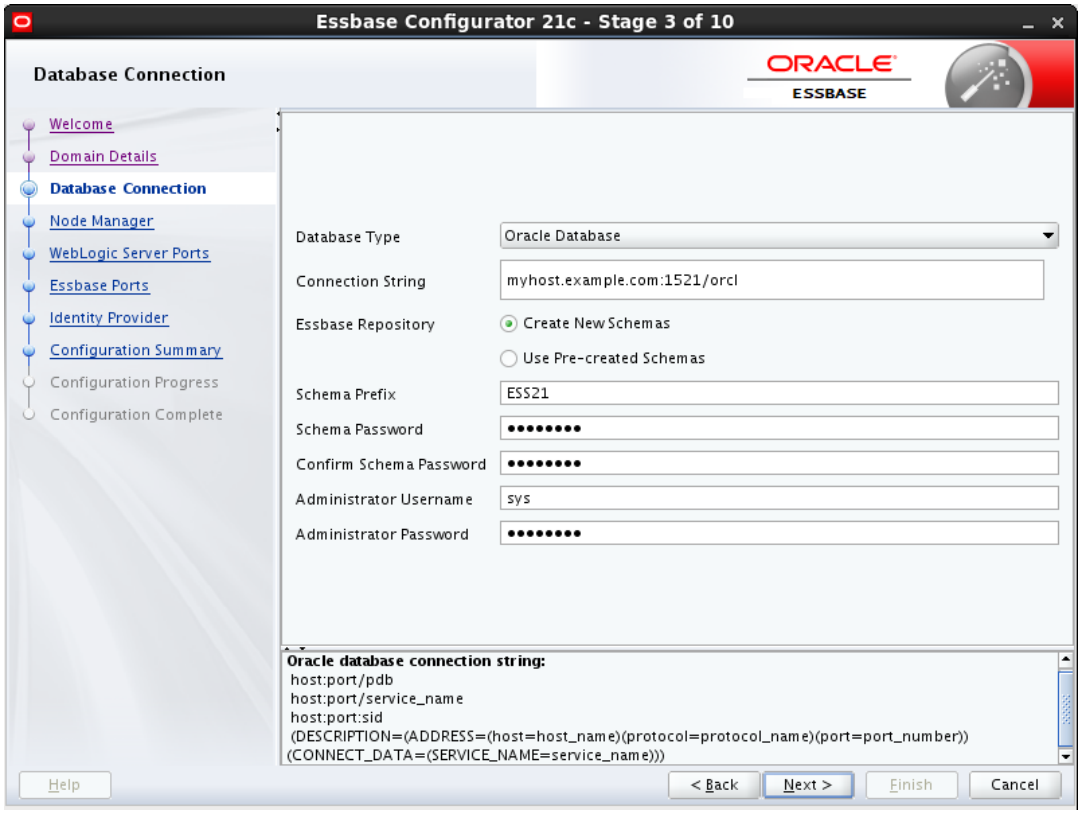
   It's recommended that the applications directory be separate from the configuration files.

d. Enter the name and password of a WebLogic administrator account that you'll use for managing Essbase and middleware servers.

   - If you use WebLogic Embedded LDAP, this administrator is also given an Essbase service administrator role.
   - If you use EPM Shared Services, this administrator is only for the Essbase domain WebLogic instance. The EPM Shared Services admin user will be provisioned with Essbase user role: Service Administrator.

e. Click **Next**.

4. On the Database Connection page, do the following.




a. Accept the default, or enter the database type. This is the supported relational database, for example, Oracle Database.

b. Enter the connection string, for example,

```
myhost.example.com:1521/orcl
```

See Connection String Formats.

c. Choose whether to create new schemas now, or use pre-created schemas that you built using Fusion Middleware RCU utility in Pre-create RCU Schemas for Essbase, as a pre-configuration workflow task. If using Microsoft SQL Server (MSSQL) in configuration, see related prerequisite above.

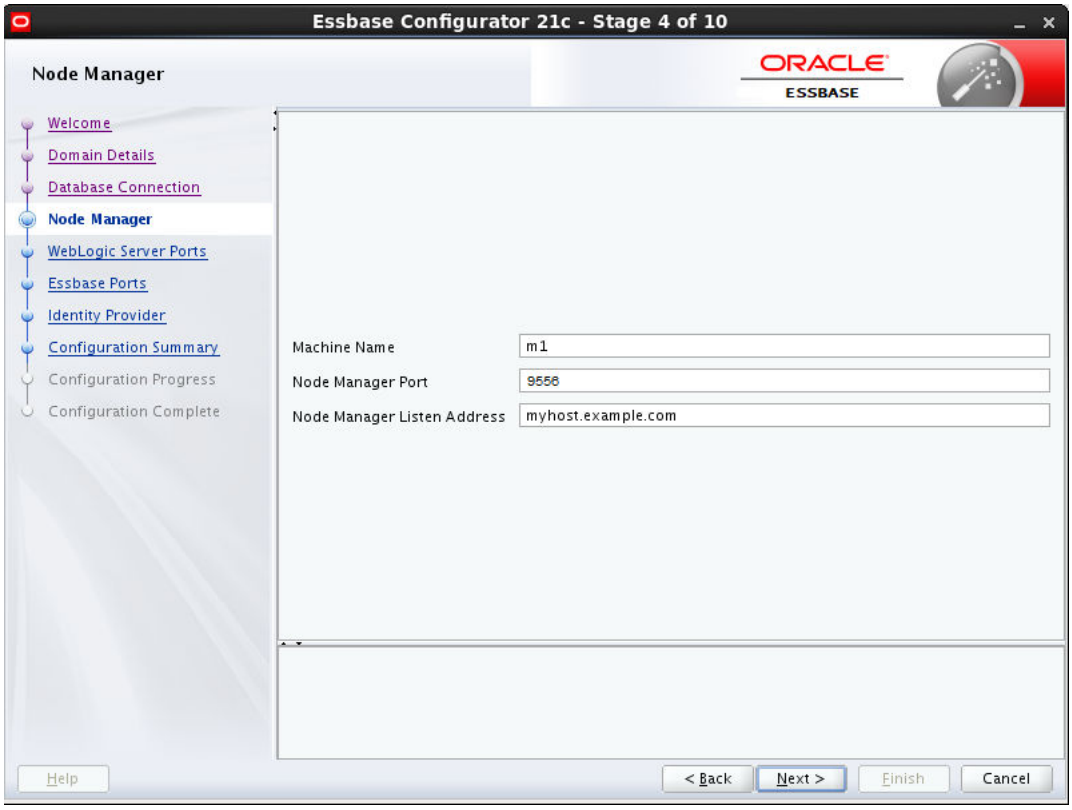
d. Enter a schema prefix, for example, ESS21C. This must be a new, unique string, containing 1-12 alphanumeric characters, and starting with a letter.

e. Enter a schema password that will be shared for all of the new schemas.

f. For the administrator username and password, enter the credentials of any user granted a sysdba role for your Oracle Database. This can be the default sys user; or Microsoft database administrator. Username must start with a letter and contain between 5 and 128 alphanumeric characters long. Password must start with a letter, contain between 8 and 30 characters long, at least one number, and, optionally any number of the special characters ($ # _).

g. Click **Next**.

5. On the Node Manager Configuration page, do the following.

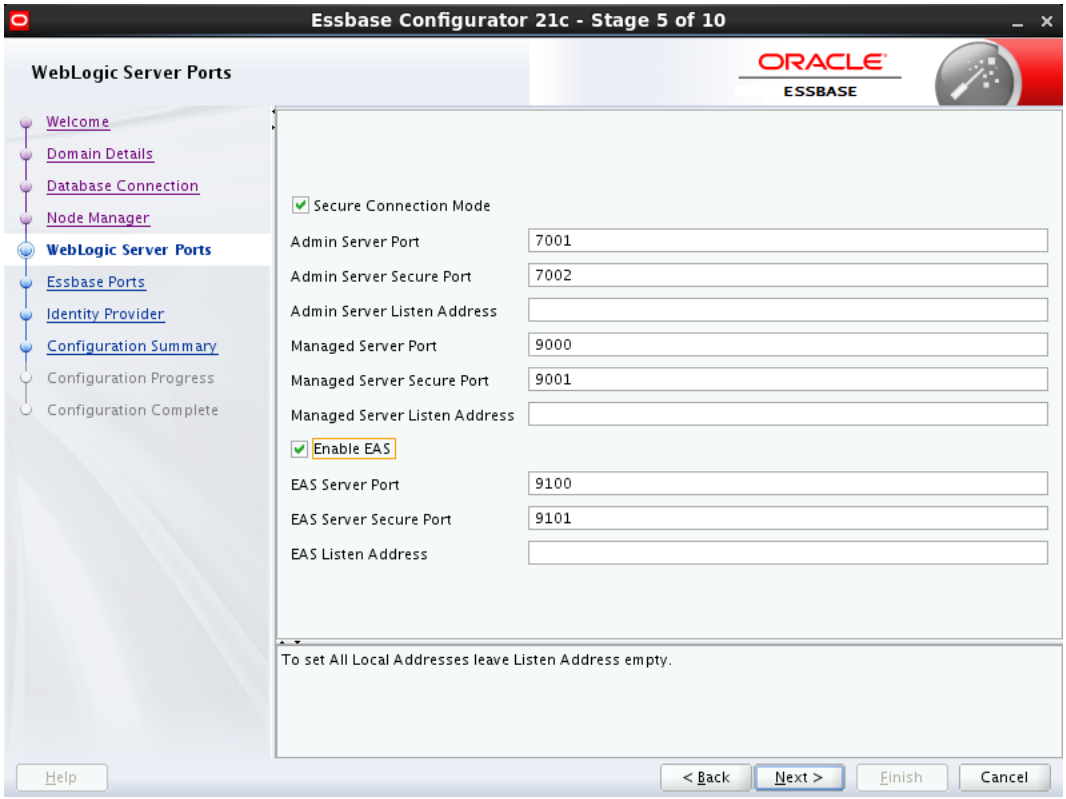



a. Accept the defaults, or enter the string for the Node Manager machine name, which handles clusters. All ports should not be within the ephemeral ports range, nor in use by other running software. See Avoid Port Conflicts.

b. For Node Manager Listen Address, you can enter your fully qualified Linux host name (where WebLogic is installed along with your Fusion Middleware installation). It can also be an operating system address. For reference, see Configure Listen Addresses.

c. Click **Next**.

6. On the WebLogic Server Ports Configuration page, configure according to the choices you made during installation.




Specify clear and secure ports for each of the servers. See Server Configuration Options. All ports should not be within the ephemeral ports range, nor in use by other running software. See Avoid Port Conflicts.

a. To secure connections using Transport Layer Security (TLS Everywhere), select the **Secure Connection Mode** check box; your self-signed certificate is then recognized. If you didn't already, review this topic: About Securing Your Communication and Network. If TLS security is deployed, the default port is the Managed Server Secure port. Default port value is 9000 for non-secured, and 9001 for secured. It is recommended to use secured (9001).

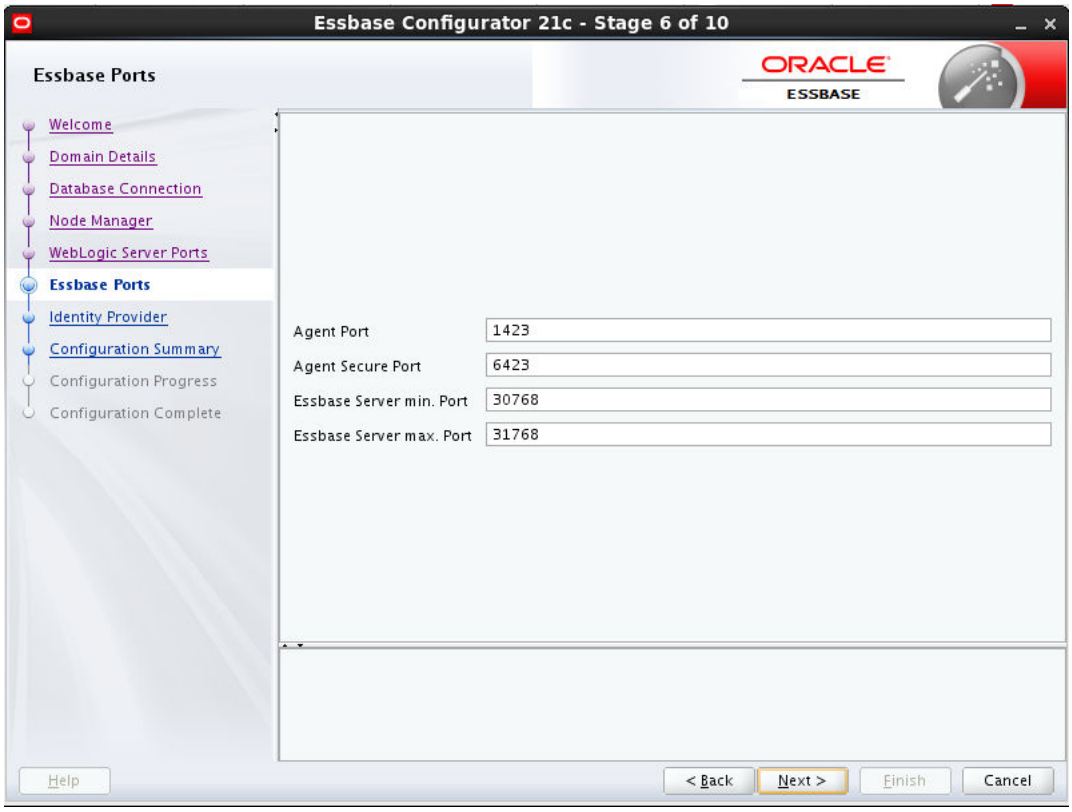
   If you configure Essbase to use a non-Oracle relational database as the RCU repository database, you may need to take additional steps, after Essbase deployment is completed, to configure your system's ODBC drivers to support secure/TLS encryption. Consult your database driver configuration instructions.

b. To manage applications using Essbase Administration Services, select **Enable EAS**. Defaults are: EAS Server Port: 9100, and EAS Server Secure Port: 9101. EAS input fields are available when **Enable EAS** is selected.

c. [Optional] To limit access to specific hosts, (for multi-home environment), specify a domain, for example, `localhost`, in the listen address fields. If you don't specify/enter listen addresses values, the listen addresses apply to all interfaces and addresses, and all mapped hosts are accessible.

d. Click **Next**.

7. On the Essbase Ports Configuration page, do the following.

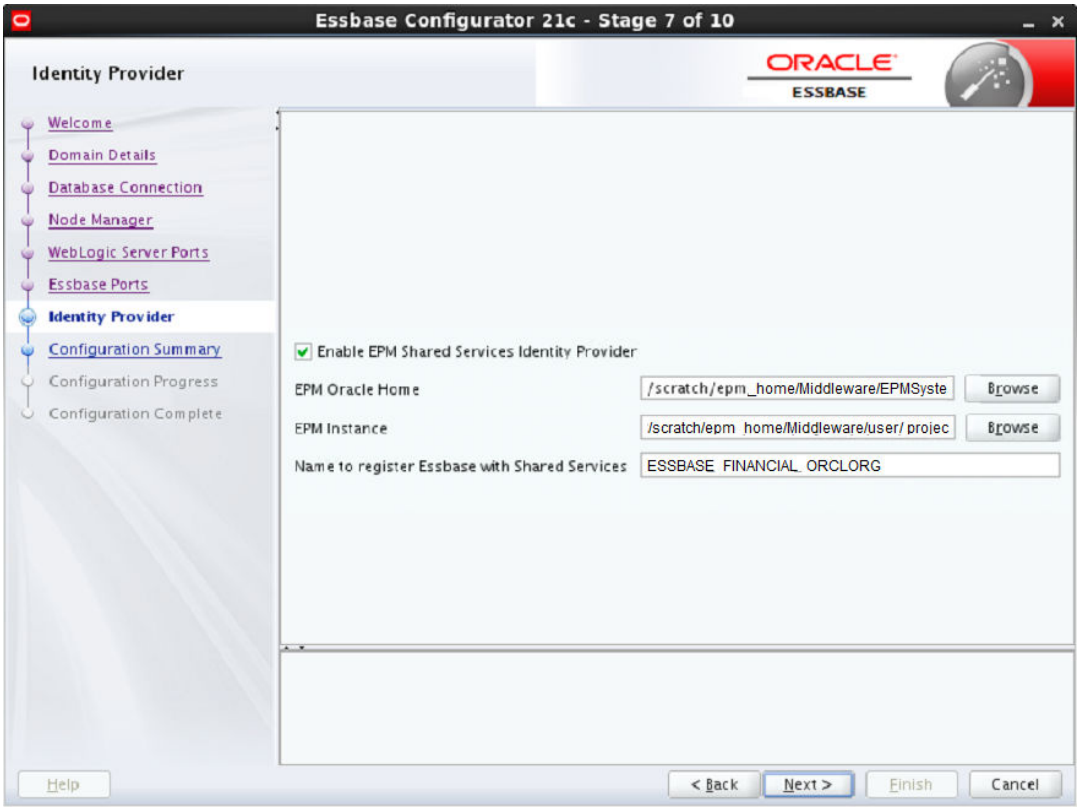



a. Accept the defaults or enter values for the Agent Port, Agent Secure Port (used for secure communication using TLS), and min and max ports for Essbase application servers.

   - Agent Port specifies the port for the Essbase Agent - default is 1423.
   - Agent Secure Port specifies the port that the Essbase Agent uses for secure communication when in secure connection mode with Transport Layer Security (TLS) - default is 6423.
   - When multiple instances of Essbase Server are installed on one host, you must specify a unique port number for each instance.
   - All ports should not be within the ephemeral ports range, nor in use by another running software. See Avoid Port Conflicts.
   - The range between Min and Max ports must be at least 1000, depending on the amount used.

b. Click **Next**.

8. On the Identity Provider configuration page, do the following.



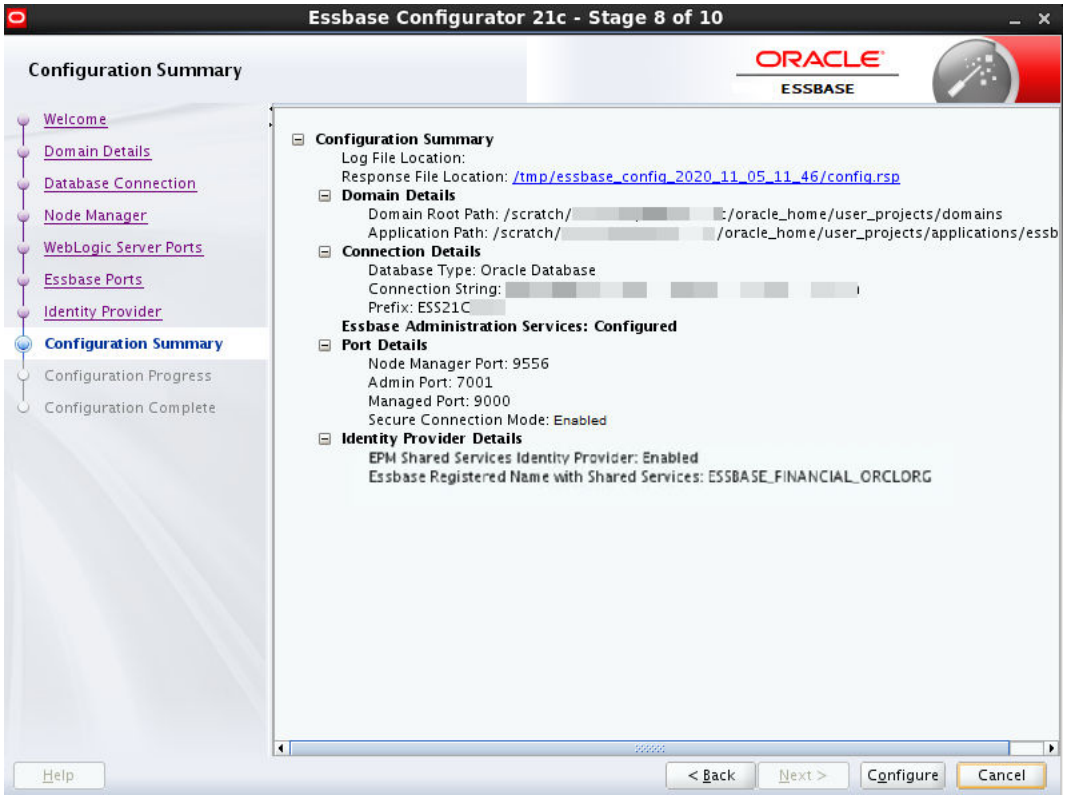

a. If you didn't already, review Select Authentication Provider topic.

b. WebLogic is the default. If you currently use EPM Shared Services, and want to continue, select the **Enable EPM Shared Services Identity Provider** check box. The window example shows EPM provider selected. When enabled, EPM fields are available for you to confirm or specify **EPM Oracle Home** and **Oracle Instance** locations. For details on these, see About Middleware Home, EPM Oracle Home, and EPM Oracle Instance.

c. [Optional] You can optionally enter a name to register the Essbase instance with Shared services. If a name is not provided, EPM generates the name for the registered instance.

d. Click **Next**.

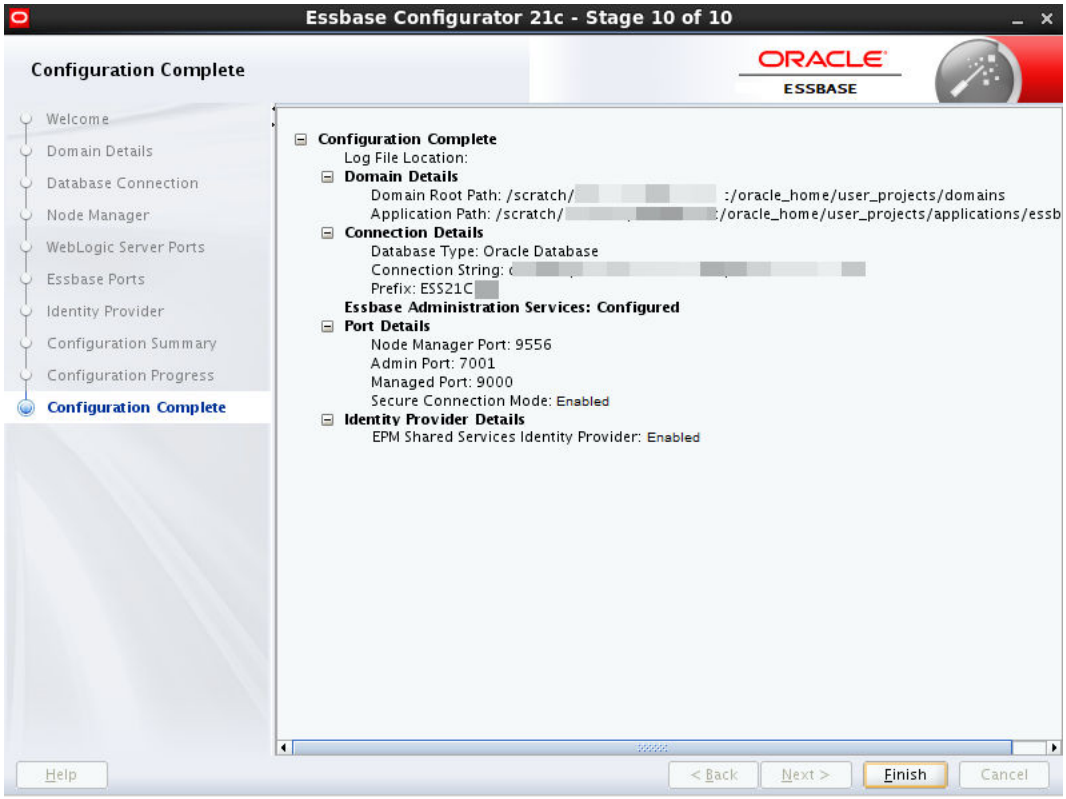
9. Review the Configuration Summary page. Note the log file location (path not shown) and response file location. This window example may vary from your selected entries or values.




You can use the response file (.rsp) to save your configuration choices and fill in the same field values (excluding passwords) in a future UI-based or Silent mode configuration. If you want to run a future configuration using an .rsp file, you can also run configuration until the summary page, and click **Cancel** instead of **Configure**, and reuse the response file later.

The .rsp file is saved at the temp location listed in the summary as Response File Location. If you plan to use it for automating a future configuration, be sure to save it somewhere more permanent, as `tmp` directories may be routinely cleaned out. See Sample Response File and Parameters.

10. Click **Configure**. On the Configuration Progress page, near the end of Configuration Tool processing, Essbase platform components are started. When progress reaches 100%, click **Next**.
11. On the Configuration Complete page, review the details, and click **Finish**. Note that this window example doesn't necessarily reflect your selected entries or values. You can now log into Essbase. See Essbase, REST, and Smart View Client URLs.




Advanced and post-configuration options and tasks can be reviewed in Advanced Configuration Topics. This includes topics on deleting RCU schemas, configuring Essbase and Oracle HTTP server, and more.

# Configure Essbase on Windows

You must configure Essbase on Windows using the Configuration Tool after installation.

**Prerequisites and Notes**

- Fusion Middleware must already be installed, and Oracle Essbase must be installed in the same Oracle Home directory. See Install Fusion Middleware.
- Supported relational database must be installed, as mentioned in the installation prerequisites. See Install a Relational Database.
- If you are using EPM Shared Services authentication, you must already have a supported version of EPM installed, with EPM users Shared Services created and configured, and know your Oracle Home and EPM instance details.
  - If using EPM Shared Services authentication, it should be running during Essbase configuration. If EPM Shared Services is not running, some port numbers must be manually configured to avoid port conflicts. When you configure Essbase, you must be cautious and aware of ports that are already in use by any EPM services on this host, and to only choose and use valid ports that are not used by a service or application on this host. You must also set these unused port numbers accordingly in the user interface or in the response file.
  - If you are using Essbase 21c versions prior to 21.2.1, use an empty EPM Foundation Services instance that is separate from your production EPM instance. EPM Server must run while you configure and run Essbase. You can connect your user

management directory service to both Foundation Shared Services deployments, and must maintain application provisioning in both Shared Services instances.

  - For versions prior to Essbase 21.2.1, you needed to install a separate EPM Foundation.
  - For versions of Essbase 21.2.1 and later, install or reuse an existing EPM 11.2.x (including 11.2.x Essbase), to be configured with 21.2.x.

- If you are using Microsoft SQL Server (MSSQL) as the database for Essbase repository (RCU) schemas, you must run the process to alter database and apply the correct collate, and address schema considerations, before running the Essbase configuration tool. For more information, see Configure Microsoft SQL Server as Repository Database for Essbase Schemas.
- Pre-create RCU Schemas for Essbase explains the process if you choose to pre-create RCU schemas before configuration rather then have Configuration Tool create them for you. One use case to pre-create schemas is if you're employing a secure HTTPS connection using a wallet.
- In Windows Control Panel > Clock and Region > Region, select Administrative tab. Click **Change System Locale** and select check box **Beta: Use Unicode UTF-8 for worldwide language support**.
- Essbase on Windows cannot have multiple configurations or instances on the same host.
- You must apply the following patches on Oracle Home before creating RCU schemas, whether or not you use pre-created schemas. Check the latest patches in the Essbase Release Notes section for Independent Deployment, or contact Support, to verify appropriate patch versions.
  - 28186730 - latest version of OPatch 13.9.4.2.x for FMW/WLS
  - 31676526 - patch 12.2.1.4.0 for TNS_ADMIN RCU warning
  - 30540494 - patch 12.2.1.4.0 for RAC RCU bug
  - 30754186 - patch 12.2.1.4.0 for RAC RCU bug
- All ports should not be within the ephemeral ports range, nor in use by other running software. See Avoid Port Conflicts.
- Each managed server must be assigned to a machine, the logical representation of the computer that hosts one or more server instances. The machine name must be unique in relation to other configurable resources in the domain.
- If you plan to install and configure more than one Essbase On-Premise instance, to support failover, you need a front-end load balancer, and the instances must be configured on different hosts. As mentioned, Essbase on Windows cannot have multiple configurations or instances on the same host. See Configure a Load Balancer to Support Failover.
- If Essbase service is to be configured or available as Essbase Windows service, to start and stop Essbase service, PowerShell must be in the environment PATH variable. You must also enable Essbase Windows Service during configuration, to install Windows service.
- If you're connecting through Smart View, using the URL `/aps/SmartView`, you need to change the URL. See Redirect to New Essbase Smart View Connection URL. Alternatively, you can configure redirection to the new URL on the web server. If you're using Oracle HTTP Server (OHS) or HTTPD Server, redirect the URL while modifying the Oracle HTTP Server configuration, as noted in the previous bullet.

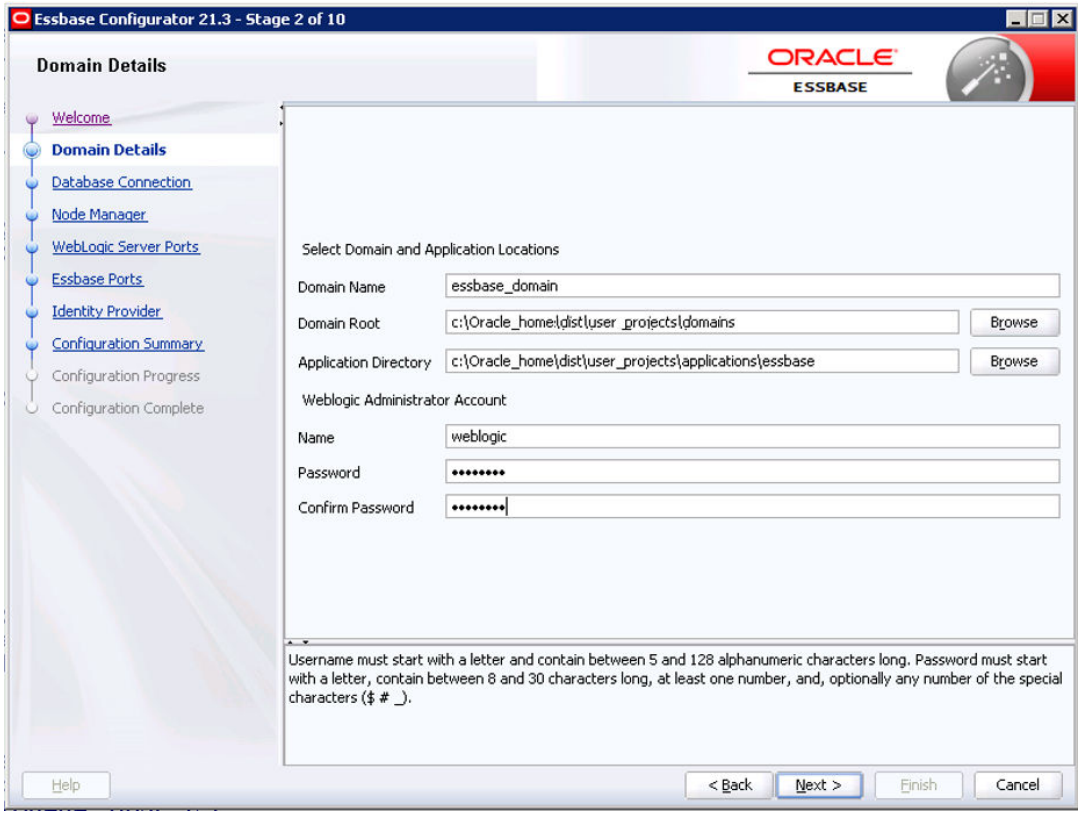
- For access to the response file, and use it, you must set TEMP and TMP environment variables for the user, as follows:
  1. On the Windows task bar, right-click the Windows icon and select **System**.
  2. In the Settings page, under Related Settings header on the right, click **Systems info** and then **Advanced System settings**.
  3. Select **Environment Variables**.
  4. Either click **New** to create new environment variables TEMP and TMP or click **Edit** to modify existing environment variables TEMP and TMP, with your user variable values. You can use the same value for both.
  5. After you set, open a new cmd or command prompt to reflect the new variable set.

### Run Configuration Tool

1. If you didn't continue with configuration at the end of installation, launch the Configuration Tool.
   a. In the Oracle Home directory, where Essbase and Fusion Middleware are installed, open a terminal in `\essbase\bin`. For example, open a terminal in `<Oracle_Home>\essbase\bin`.
   b. Launch the Configuration Tool using the config.cmd command script.

      ```
      config.cmd
      ```

      The script can be run with parameters (such as -mode, -log, -log priority, -responseFile). If you use the responseFile parameter, all fields are filled with previous configuration entries, except for passwords. To learn about configuration script options, run: `config.cmd -help`.
2. On the Welcome page, click **Next**.
3. On the Domain Details page, do the following.




a. Accept the default (if correct) or enter your domain name, for example, `essbase_domain`.

b. Accept the default (if correct) or enter your domain root path, for example,

   ```
   C:\Oracle_home\dist\user_projects\domains
   ```

c. Accept the default or enter your application directory, for example,

   ```
   C:\Oracle_home\dist\user_projects\applications\essbase
   ```

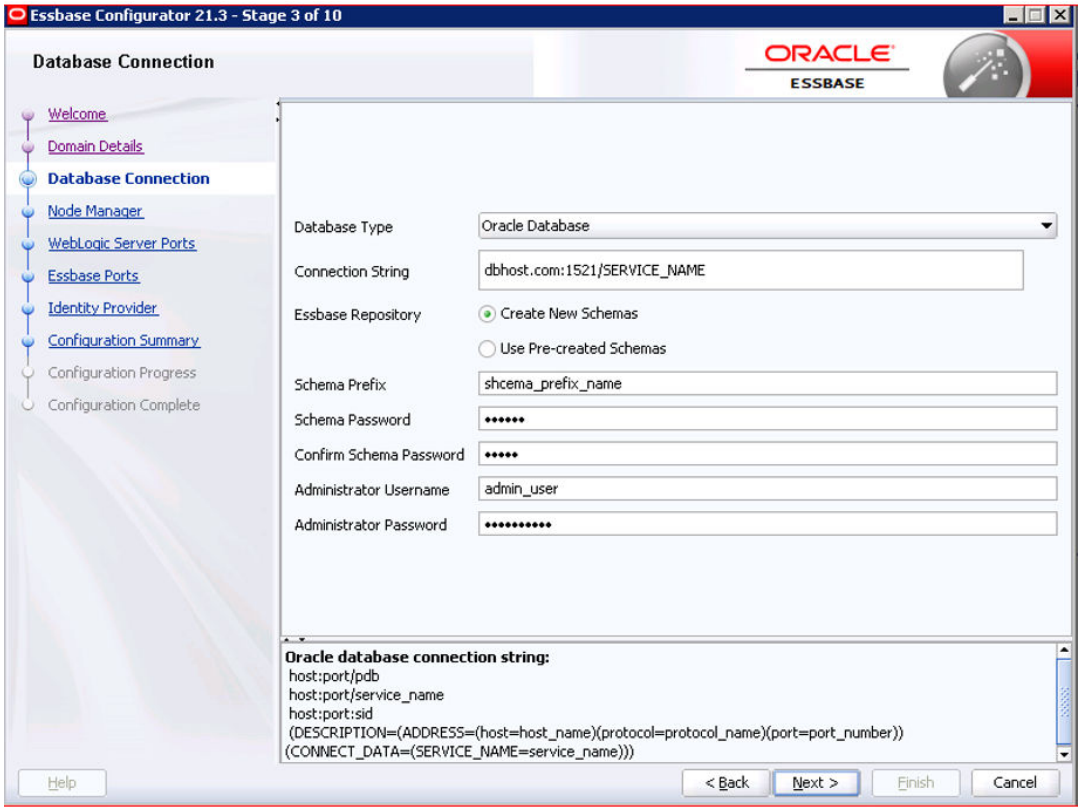
   It's recommended that the applications directory be separate from the configuration files.

d. Enter the name and password of a WebLogic administrator account that you'll use for managing Essbase and middleware servers.

   - If you use WebLogic Embedded LDAP, this administrator is also given an Essbase service administrator role.
   - If you use EPM Shared Services, this administrator is only for the Essbase domain WebLogic instance. The EPM Shared Services admin user will be provisioned with Essbase user role: Service Administrator.

e. Click **Next**.

4. On the Database connection page, do the following.




a. Accept the default, or enter the database type. This is the supported relational database, for example, Oracle Database.

b. Enter the connection string, for example,

```
myhost.example.com:1521/orcl
```

See Connection String Formats.

c. Choose whether to create new schemas now, or use pre-created schemas that you built using Fusion Middleware RCU utility in Pre-create RCU Schemas for Essbase, as a pre-configuration workflow task. If using Microsoft SQL Server (MSSQL) in configuration, see related prerequisite above.

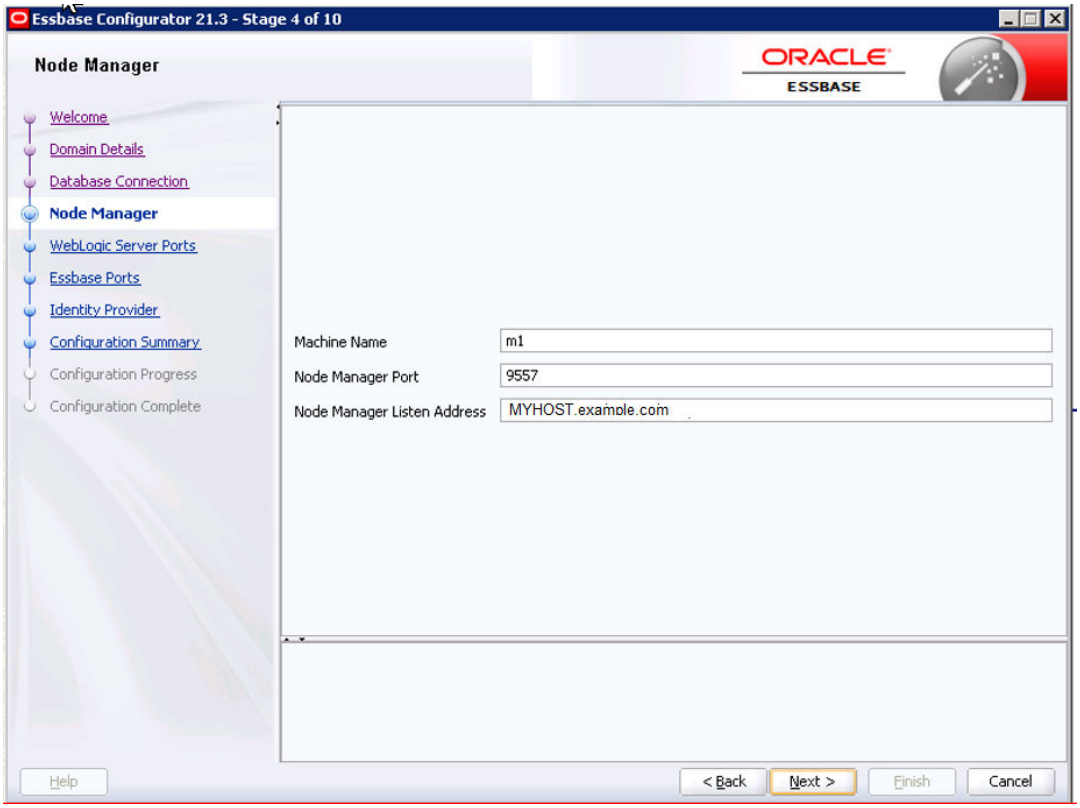
d. Enter a schema prefix, for example, ESS21C. This must be a new, unique string, containing 1-12 alphanumeric characters, and starting with a letter.

e. Enter a schema password that will be shared for all of the new schemas.

f. For the administrator username and password, enter the credentials of any user granted a sysdba role for your Oracle Database. This can be the default sys user; or Microsoft database administrator. Username must start with a letter and contain between 5 and 128 alphanumeric characters long. Password must start with a letter, contain between 8 and 30 characters long, at least one number, and, optionally any number of the special characters ($ # _).

g. Click **Next**.

5. On the Node Manager Configuration page, do the following.

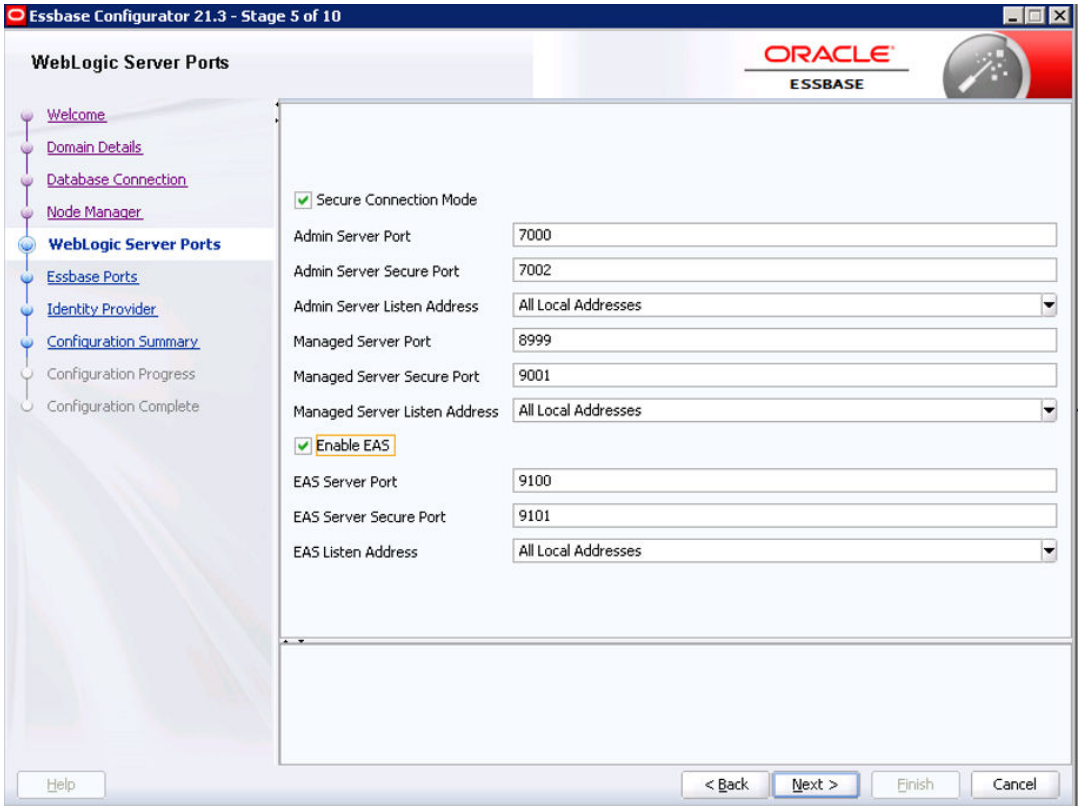



a. Accept the defaults, or enter the string for the Node Manager machine name, which handles clusters. All ports should not be within the ephemeral ports range, nor in use by other running software. See Avoid Port Conflicts.

b. For Node Manager Listen Address, you can enter or select your fully qualified host name (where WebLogic is installed along with your Fusion Middleware installation). It can also be an operating system address. For reference, see Configure Listen Addresses.

c. Click **Next**.

6. On the WebLogic Server Ports Configuration page, configure according to the choices you made during installation.




Accept the defaults or enter values. Values in the above screen are only examples. Specify clear and secure ports for each of the servers. See Server Configuration Options. All ports should not be within the ephemeral ports range, nor in use by other running software. See Avoid Port Conflicts.

a. To secure connections using Transport Layer Security (TLS Everywhere), select the **Secure Connection Mode** check box; your self-signed certificate is then recognized. If you didn't already, review this topic: About Securing Your Communication and Network. If TLS security is deployed, the default port is the Managed Server Secure port. Default port value is 9000 for non-secured, and 9001 for secured. It is recommended to use secured (9001).

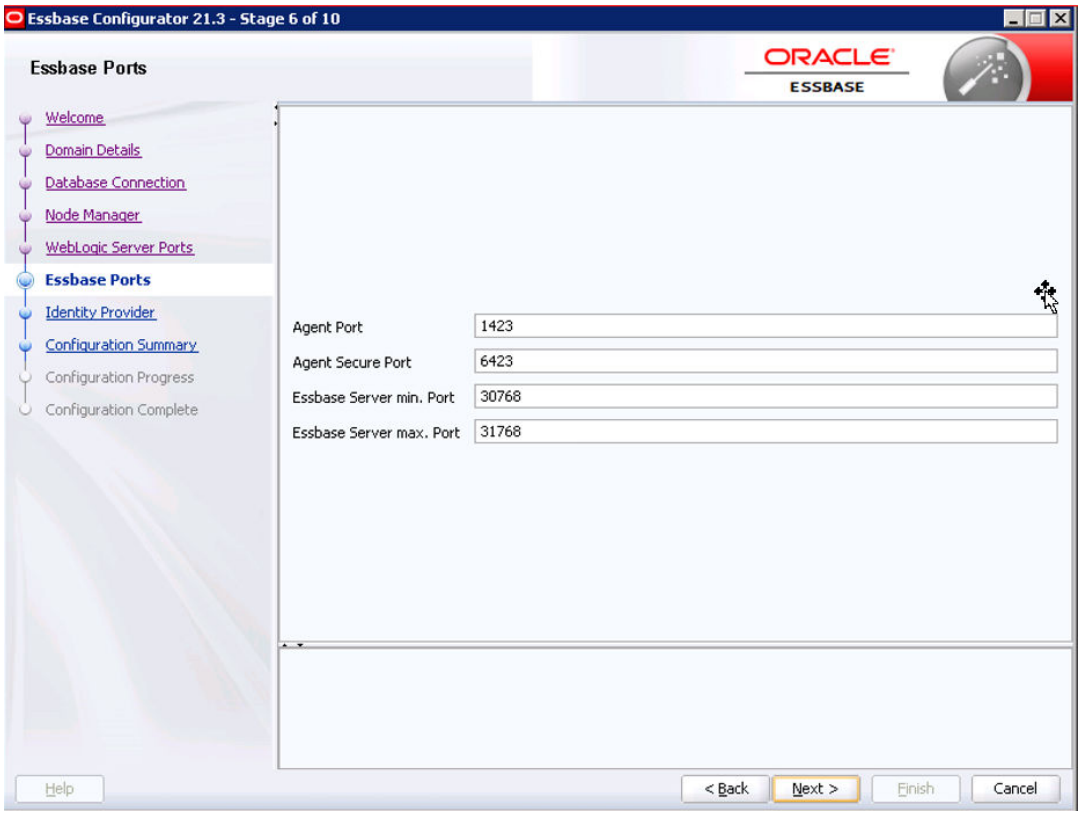
   If you configure Essbase to use a non-Oracle relational database as the RCU repository database, you may need to take additional steps, after Essbase deployment is completed, to configure your system's ODBC drivers to support secure/TLS encryption. Consult your database driver configuration instructions.

b. To manage applications using Essbase Administration Services, select **Enable EAS**. Defaults are: EAS Server Port: 9100, and EAS Server Secure Port: 9101. EAS input fields are available when **Enable EAS** is selected.

c. [Optional] To limit access to specific hosts (for multi-home environment), specify or select a domain, for example, `localhost`, in the listen address fields. If you don't select/enter listen addresses values, the listen addresses apply to all interfaces and addresses, and all mapped hosts are accessible.

d. Click **Next**.

7. On the Essbase Ports Configuration page, do the following.

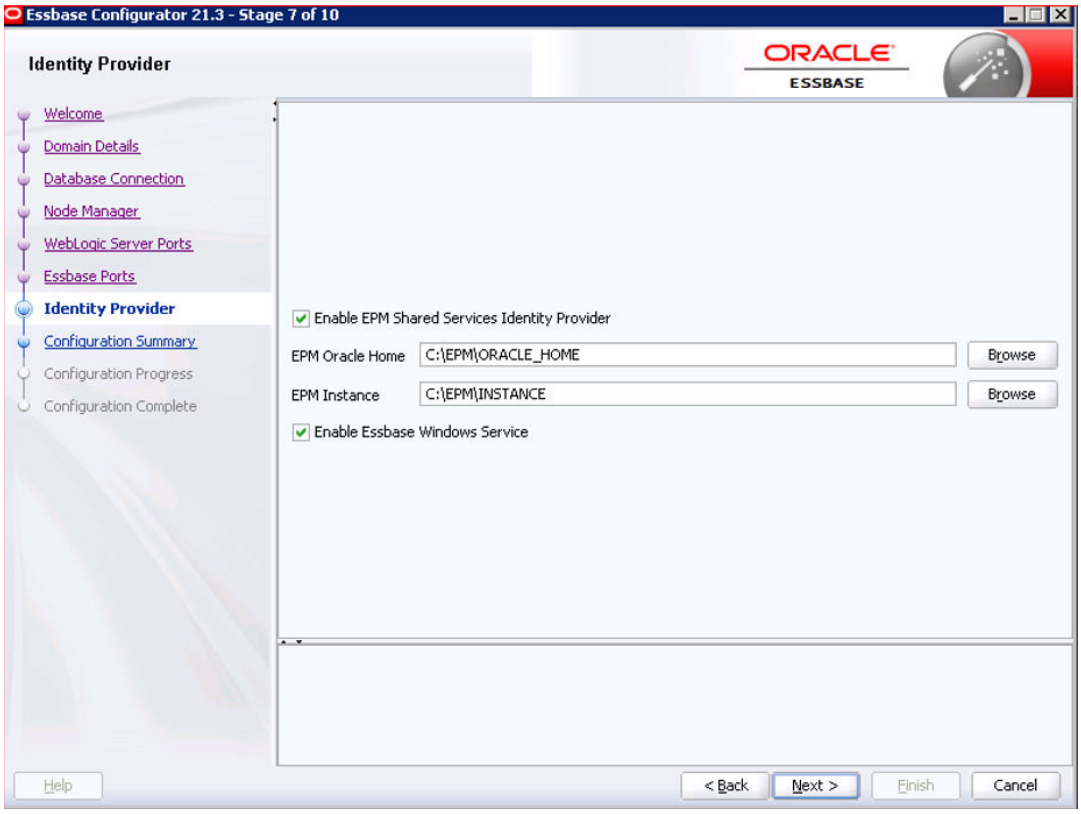



a. Accept the defaults or enter values for the Agent Port, Agent Secure Port (used for secure communication using TLS), and min and max ports for Essbase application servers.

   - Agent Port specifies the port for the Essbase Agent - default is 1423.
   - Agent Secure Port specifies the port that the Essbase Agent uses for secure communication when in secure connection mode with Transport Layer Security (TLS) - default is 6423.
   - When multiple instances of Essbase Server are installed on one host, you must specify a unique port number for each instance.
   - All ports should not be within the ephemeral ports range, nor in use by another running software. See Avoid Port Conflicts.
   - The range between Min and Max ports must be at least 1000, depending on the amount used.

b. Click **Next**.

8. On the Identity Provider configuration page, do the following.



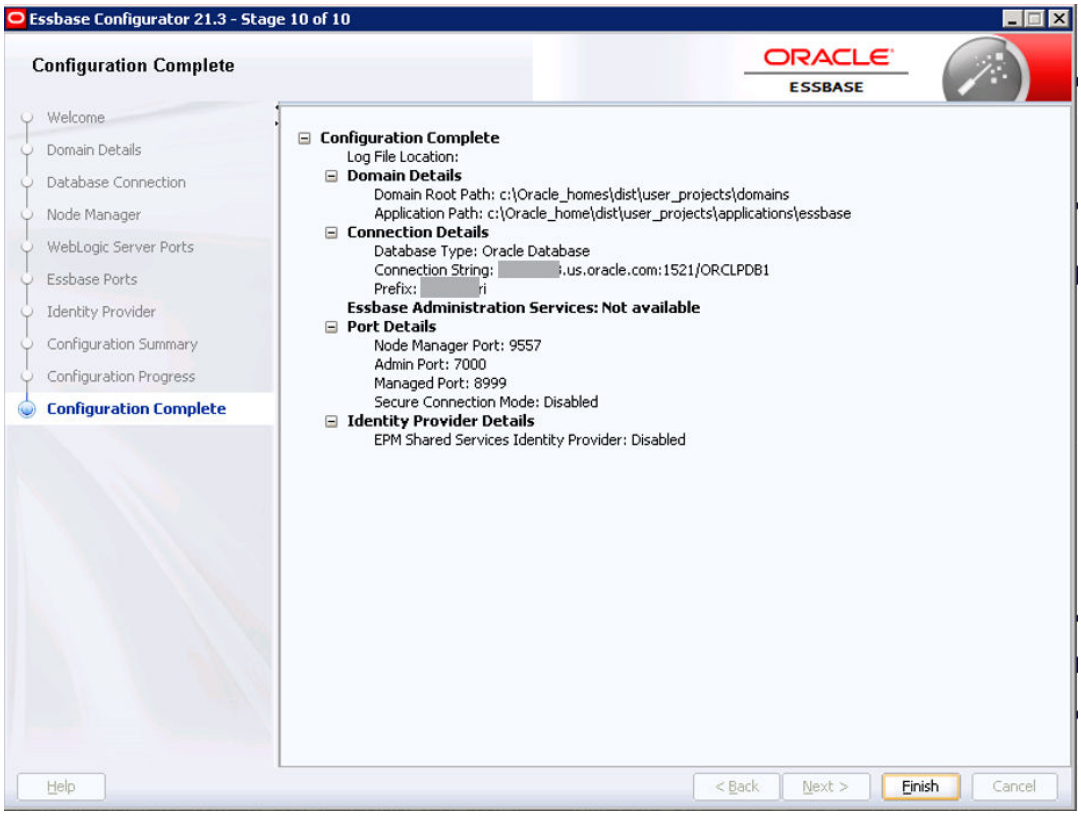

a. If you didn't already, review Select Authentication Provider topic.

b. WebLogic is the default. If you currently use EPM Shared Services, and want to continue, select the **Enable EPM Shared Services Identity Provider** check box. The window example shows EPM provider selected. When enabled, EPM fields are available for you to confirm or specify **EPM Oracle Home** and **Oracle Instance** locations. For details on these, see About Middleware Home, EPM Oracle Home, and EPM Oracle Instance.

c. For Essbase Windows service to be configured or available, to start and stop Essbase service, PowerShell must be in environment variable PATH. You must also enable Essbase Windows Service during configuration, to install Windows service. To use this feature, you must select **Enable Essbase Windows Service**, on this page, to install Windows service. Start and stop of the Essbase Windows Service is done using Windows SCM.

d. Click **Next**.

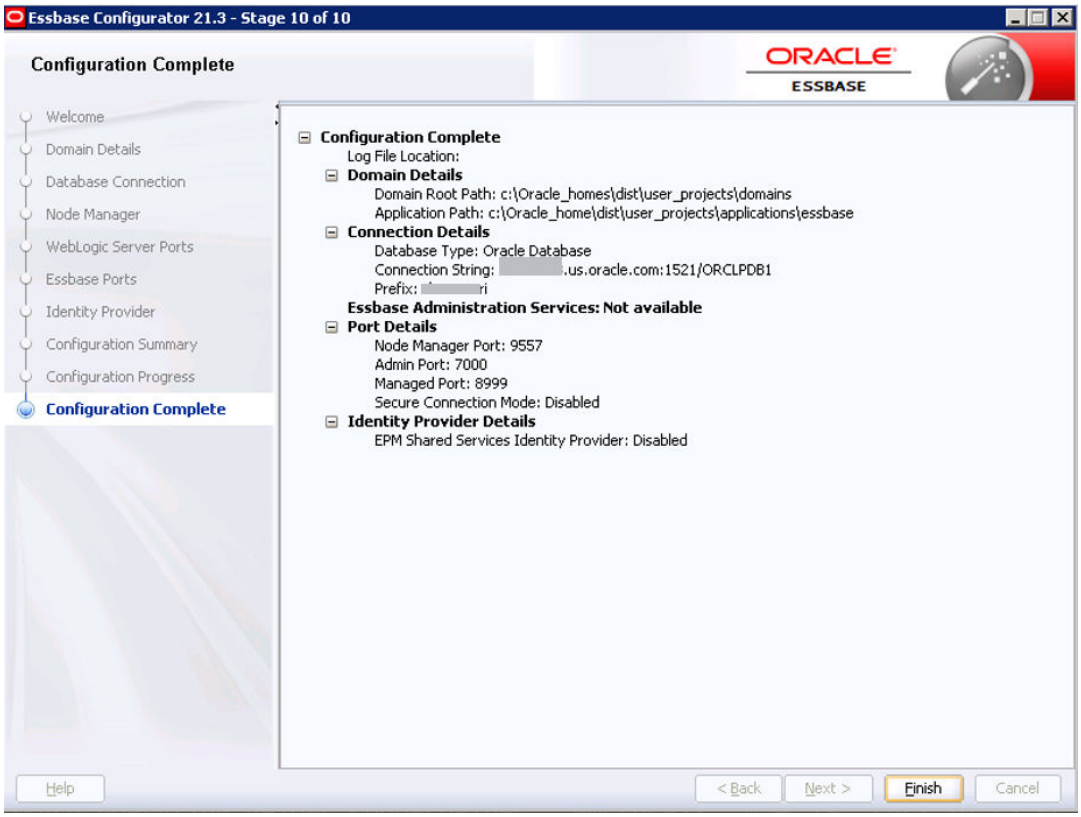
9. Review the Configuration Summary page. Note the log file location (if shown) and response file location. This window example may vary from your selected entries or values.




You can use the response file (.rsp) to save your configuration choices and fill in the same field values (excluding passwords) in a future UI-based or Silent mode configuration. If you want to run a future configuration using an .rsp file, you can also run configuration until the summary page, and click **Cancel** instead of **Configure**, and reuse the response file later.

The .rsp file is saved at the temp location listed in the summary as Response File Location. If you plan to use it for automating a future configuration, be sure to save it somewhere more permanent, as `tmp` directories may be routinely cleaned out. See Sample Response File and Parameters.

10. Click **Configure**. On the Configuration Progress page, near the end of Configuration Tool processing, Essbase platform components are started. When progress reaches 100%, click **Next**.
11. On the Configuration Complete page, review the details, and click **Finish**. Note that this window example doesn't necessarily reflect your selected entries or values. You can now log into Essbase. For login URLs, see Essbase, REST, and Smart View Client URLs.




**Note:**

If you configured Essbase securely with an external database using a TNS_ADMIN alias, for example, `adwsql_low?TNS_ADMIN=C:/Users/opc/Documents/EssbaseADWS`, you must do the following so that the connection can be processed by the Essbase server:

a. Edit:

```
<DOMAIN_HOME>\bin\setStartupEnv.cmd
```

b. Add the following line to the startup script, before `-DODBC_URL=` usage:

```
set TNS_ADMIN=C:/Users/opc/Documents/EssbaseADWS
```

c. Change the following line:

```
-DODBC_URL='OCI;SERVICE=adwsql_low?TNS_ADMIN=C:/Users/opc/
Documents/EssbaseADWS'
```

to

```
-DODBC_URL='OCI;SERVICE='adwsql_low'
```

Advanced and post-configuration options and tasks can be reviewed in Advanced Configuration Topics. This includes topics on deleting RCU schemas, configuring Essbase and Oracle HTTP server, and more.

# Run Oracle Essbase Configuration in Silent Mode

Oracle Essbase can be configured using Silent Mode.

You can use the predefined values in the response file, or edit it and specify variable values. If variables aren't included in the response file, system default values are used.

See the Prerequisites and Notes in Configure Essbase on Linux.

**Run Silent Mode Configuration**

1. To get a formatted .rsp (response) file for Silent mode configuration, run the Configuration Tool to generate it. Run Configuration Tool only until Configuration Summary page, save the listed .rsp file, and then click **Cancel** from the Configuration Tool, instead of **Configure**.
2. When you use the response file, all fields are filled with previous configuration entries, except for passwords. You can edit the response file, as needed, and modify parameters values, as listed in Sample Response File and Parameters.
3. Run the following command, pointing to the response file you just edited. You can run any number of similar or different configurations.
   **For Linux:**

   ```
   <Oracle_Home>/essbase/bin/config.sh -mode=silent -responseFile=<response
   file>
   ```

   For example:

   ```
   config.sh -mode=silent -responseFile=${modifiedConfigXML}
   << "EOL"
   adminPassword
   dbPASSWORD
   dbSysPassword
   EOL
   ```

   **For Windows:**

   ```
   <Oracle_Home>/essbase/bin/config.cmd -mode=silent -responseFile=<response
   file>
   ```

   For example:

   ```
   echo adminpassword^&echo dbPassword^&echo dbSyspassword^&rem.) |
   config.cmd -mode=silent -responseFile=C:\config.rsp
   ```

4. After the response file is read, and variable parameters are validated, configuration is executed. Password prompts are displayed for WebLogic admin and RDBMS schema. If `CREATE_DATABASE_SCHEMA` is set to `CREATE`, there's also a prompt for Database admin password. Alternatively, you can send passwords to the configuration using redirection in a bash script, as shown in the examples above, for complete silent mode. After configuration, you can proceed to other setup tasks.

# Advanced Configuration Topics

These are advanced configuration and post-configuration tasks.

- Pre-create RCU Schemas for Essbase
- Sample Response File and Parameters
- Delete RCU Schemas for Essbase
- Essbase Server Configuration File (essbase.cfg)
- Configure a Load Balancer to Support Failover
- Modify CRASHDUMP Configuration
- Redirect to New Essbase Smart View Connection URL
- Expand Limit for SQL IN Clauses in Drill Through Reports
- Configure Essbase Servers in a Failover Cluster
- Connection String Formats
- Environment Locations in the Essbase Platform
- Connect to Multiple Essbase 21c Servers in Shared Services and Administration Services
- Configure Microsoft SQL Server as Repository Database for Essbase Schemas

## Pre-create RCU Schemas for Essbase

Essbase platform requires the use of Repository Creation Utility (RCU) schemas for metadata storage.

Use this utility to add or drop a repository (schema).

These schemas are stored in the supported relational database of your choosing. Note that your Essbase applications and cubes are not stored in these schemas; rather, they're in your selected <Application Directory> location on the server where you install Essbase. For more information, see Plan Your Essbase Environment.

**Prerequisites**

- You must apply the patches listed as Prerequisites in Configure Essbase on Linux before creating RCU schemas, whether or not you use pre-created schemas.
- If using Microsoft SQL Server (MSSQL) in configuration, you must address the following configuration prerequisite to run the process to ALTER DATABASE and apply the correct collation, and address schema considerations. See Configuring a Microsoft SQL Server Database for the Metadata Services (MDS) Schema.
- Fusion Middleware was installed. See Install Fusion Middleware.
- Supported relational database was installed. See Install a Relational Database.
- Oracle Essbase must be present on your system before you add or drop a schema. See Install Oracle Essbase.
- Oracle recommends deploying a distinct pluggable database (PDB) for Essbase. You can read about Oracle's multitenant architecture here: Introduction to Multitenant Architecture.
  - No other applications should have access to the Essbase repository schemas generated by the Repository Creation Utility (RCU).

  - No one else other than the designated administrator should have permission to access the schemas or their tables.
  - No one else should have the credentials to assign or change roles to access the PDB.
  - Every change to the PDB should be logged.

Nine RCU schemas are currently required for Essbase and other platform components. When you configure Essbase, you can either

- use pre-created schemas, or
- let the Essbase configuration utility create them for you

The following explains how to pre-create RCU schemas using Repository Creation Utility, which is part of Fusion Middleware, instead of letting the Essbase configuration utility create them for you. Pre-creating your own schemas may be useful when you're:

- employing secure HTTPS connection using a wallet
- configuring Essbase, and then you only need to provide the schema prefix

**To pre-create RCU schemas**

1. In Oracle Home, where Fusion Middleware is installed, open a terminal in `/oracle_common/bin`, and run the `rcu` command to launch the Repository Creation Utility.

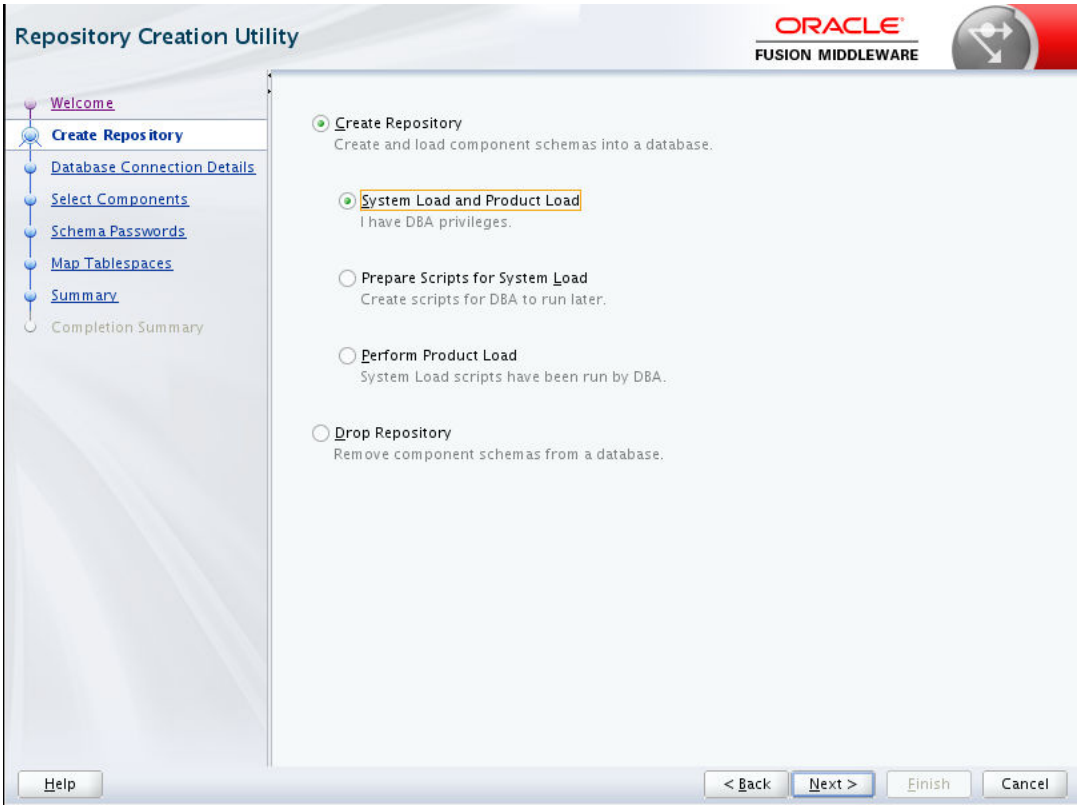
   **For Linux**

   ```
   /scratch/user/oracle_home/oracle_common/bin/rcu
   ```

   **For Windows**

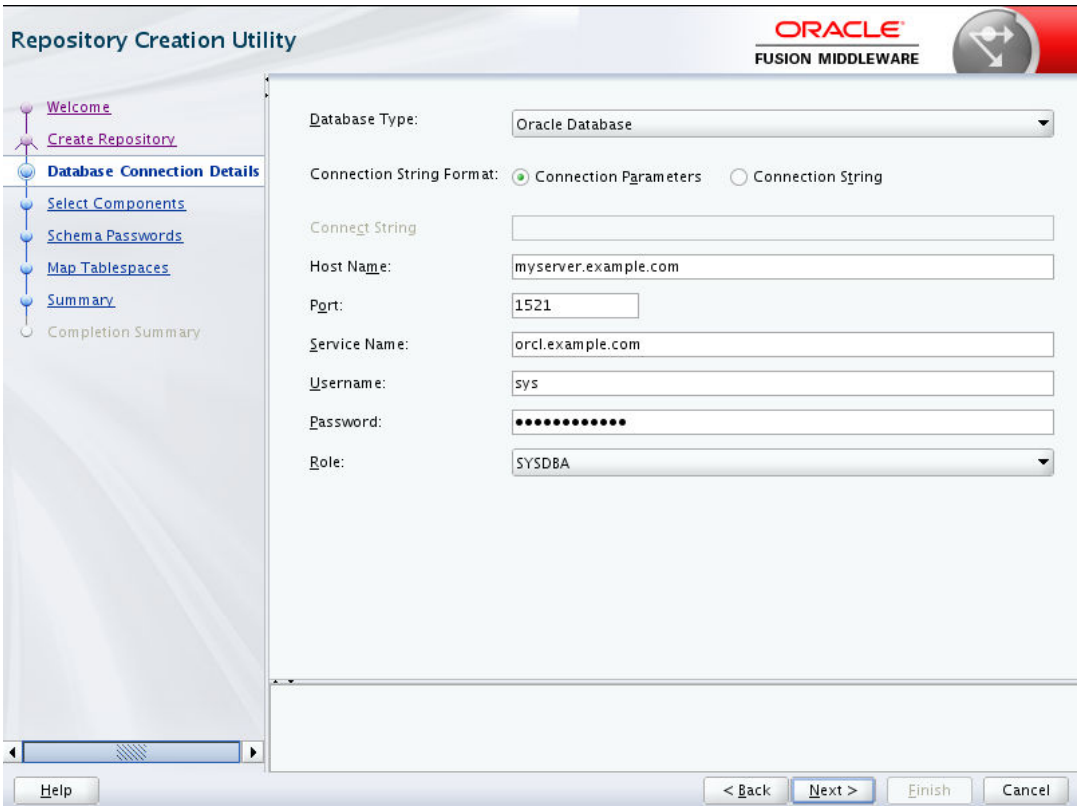
   ```
   C:\scratch\user\dist\oracle_common\bin\rcu.exe
   ```

2. On the Welcome page, click **Next**.
3. On the Create Repository page, click **Create Repository**, and click **System Load and Product Load**.




Click **Next**.

4. On the Database Connection Details page, leave **Connection Parameters** selected:

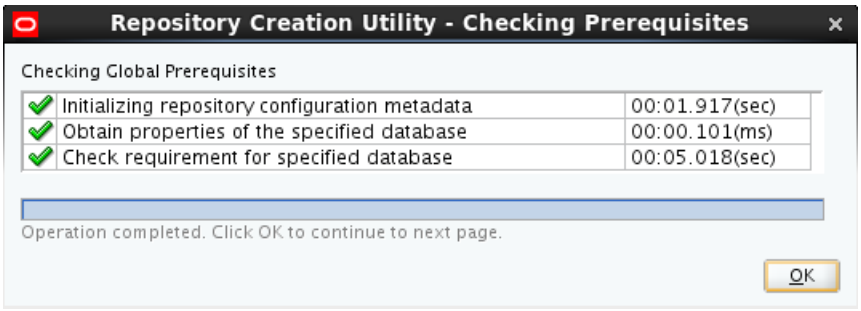


a. Enter options and values:

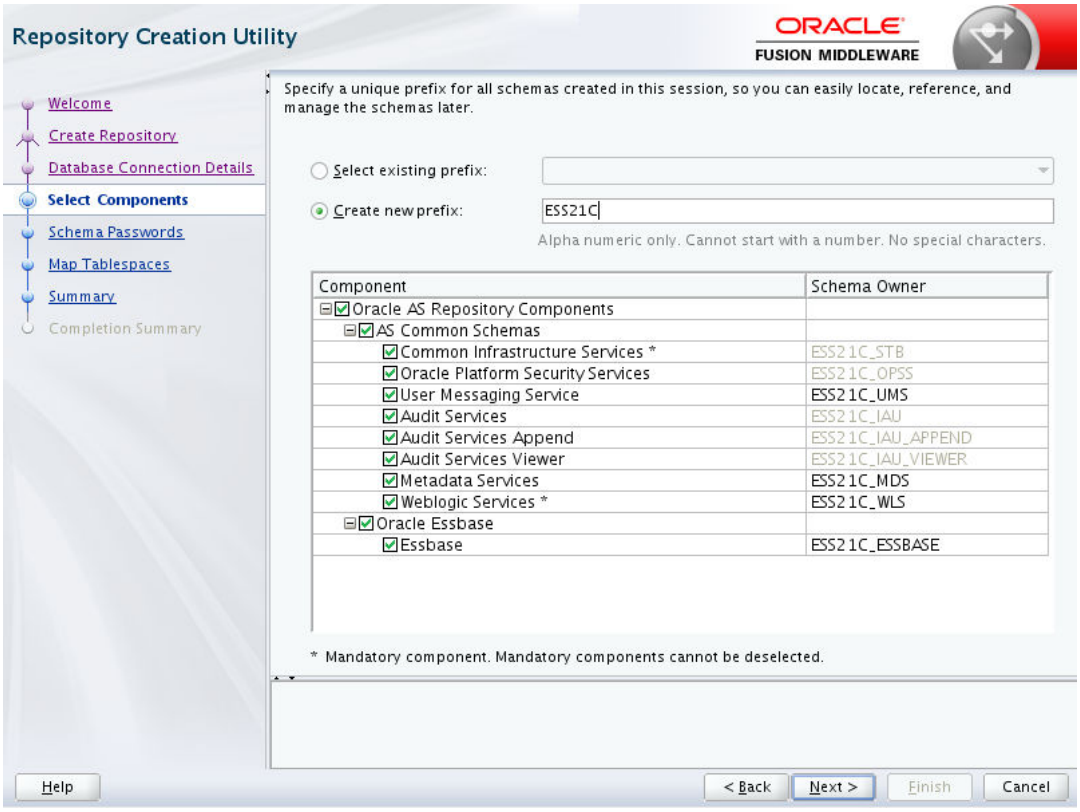
- Connection String Format - select whether to enter parameters values or use a connection string
- Host Name - fully qualified name of your server (for example, myserver.example.com)
- Port - for the Oracle Database (default is 1521)
- Service Name - for Oracle Database (for example, orcl.example.com)
- Username and Password - for Oracle Database administrator (default administrator user name may be **sys**)
- Role - leave as default of SYSDBA

b. Click **Next**.

5. The Repository Creation Utility checks prerequisites. Click **OK** to continue.




6. On Select Components page, do the following.




a. Create a new prefix; for example, ESS21C. The prefix must be unique in your database.

b. Select to create schemas for all components. Oracle Essbase and Essbase schema will NOT appear if Essbase hasn't been installed as suggested in the prerequisites.

c. Click **Next**.

7. On Schema Passwords page, enter passwords for the schemas (one shared password). Click **Next**.
8. On Map Tablespaces page, review the tablespaces and click **Next**.
9. Click **OK** to approve creation of new tablespaces in the repository database.
10. Review the Summary page. Optionally, click **Save Response File** to save your metadata and choices for reuse. Click **Create**.
11. Wait until Repository Creation Utility completes loading of schemas into the repository.
12. Review the Completion Summary. If status was **Success** for all components, click **Close**, otherwise, address any issues.
13. You have completed pre-creating schemas for Essbase and platform components. Now you're ready to configure Essbase.

**To drop a schema**

If you need to delete a repository (schema), or to clean up your Essbase schemas after an uninstall of Essbase, use this same utility. See Delete RCU Schemas for Essbase.

# Sample Response File and Parameters

Here's a list of Response file (.rsp file) variables and a sample Response file. The file can be edited and used for Configuration Tool or Silent mode configuration, and for filling in data fields based on a previous configuration.

**Table 4-1 Response File Variables**

| Variable Name | Description | Default Value | Notes |
|---|---|---|---|
| DOMAIN_NAME | Domain name | essbase_domain | Name of WebLogic Server domain you specify during configuration. |
| DOMAIN_ROOT | Domains location | - | Path in which WebLogic Server domains and configuration artifact are stored. Oracle recommends keeping it separate from the <Application Directory> and the <Oracle Home>. |
| ARBORPATH | Essbase application path | - | - |
| ADMIN_USERNAME | Admin user name of WebLogic | - | For WebLogic, administrator account that you'll use for managing Essbase and middleware servers. For EPM Shared Services, this administrator is only for the Essbase domain WebLogic instance. The Shared Services admin user will be provisioned with Essbase user role “Service Administrator." Username must start with a letter and contain between 5 and 128 alphanumeric characters long. |
| DATABASE_TYPE | Driver name of database | DB_ORACLE | Supported relational database. Available values: DB_ORACLE and DB_SQLSERVER. |
| DATABASE_CONNECT_STRING | Connection string for database connection | - | Formats of connection string: host:port/pdb, host:port/sid, host:port/service_name, (description,,,), MS SQL Server connection string: host:port:database. |

**Table 4-1 (Cont.) Response File Variables**

| Variable Name | Description | Default Value | Notes |
|---|---|---|---|
| CREATE_DATABASE_SCHEMA | Essbase RDBMS schemas | CREATE | Available values are CREATE and USE_EXISTING. CREATE option runs the repository creation tool on a prefix that doesn't exist in the database. USE_EXISTING mode uses the existing schemas. Schemas shouldn't be used in the domain. |
| DATABASE_PREFIX | Prefix for database schema | - | Prefix name must be 1-12 alphanumeric characters long, and start with a letter. |
| SECURE_MODE | True if use secure connection | - | Enables Transport Layer Security (TLS) Everywhere secure communication |
| MACHINE_NAME | WebLogic Machine name | m1 | Must be unique in relation to other configurable resources in the domain. |
| NODE_MANAGER_PORT | Port of WebLogic Node Manager | 9556 | Ports should not be within the ephemeral ports range, nor in use by other running software. See Avoid Port Conflicts . |
| NODE_MANAGER_LISTEN_ADDRESS | Listen address of WebLogic Node Manager | Fully qualified domain name | Fully qualified host name (where WebLogic is installed along with your Fusion Middleware installation). It can also be an operating system address. |
| ADMIN_SERVER_PORT | Port of AdminServer | 7001 | Ports should not be within the ephemeral ports range, nor in use by other running software. |
| ADMIN_SERVER_SSL_PORT | Secure port of AdminServer | 7002 | Port should not be within the ephemeral ports range, nor in use by other running software. |
| ADMIN_SERVER_LISTEN_ADDRESS | Listen address of AdminServer | - | Empty string means "All local addresses." To limit access to specific hosts, specify a domain. |

**Table 4-1 (Cont.) Response File Variables**

| Variable Name | Description | Default Value | Notes |
|---|---|---|---|
| MANAGED_SERVER_PORT | Port of Essbase Managed server | 9000 | Ports should not be within the ephemeral ports range, nor in use by other running software. |
| MANAGED_SERVER_SSL_PORT | Secure port of Essbase Managed server | 9001 | Ports should not be within the ephemeral ports range, nor in use by other running software. |
| MANAGED_SERVER_LISTEN_ADDRESS | Listen address of Managed server | - | Empty string means "All local addresses." To limit access to specific hosts, specify a domain. |
| ENABLE_EAS | If, true enables use of Essbase Administration Services (EAS) Lite | false | Enable use of EAS Lite to manage applications. |
| AGENT_PORT | Port of Essbase Java Agent (JAgent) | 1423 | Ports should not be within the ephemeral ports range, nor in use by other running software. |
| AGENT_SSL_PORT | Secure port of Essbase Java Agent (JAgent) | 6423 | Used for secure communication using TLS. Ports should not be within the ephemeral ports range, nor in use by other running software. |
| ESSBASE_SERVER_MIN_PORT | Minimal port of Essbase Server connection | 30768 | The range between Min and Max ports must be at least 1000, depending on the amount used. Ports should not be within the ephemeral ports range, nor in use by other running software. |
| ESSBASE_SERVER_MAX_PORT | Maximal port of Essbase Server connection | 31768 | The range between Min and Max ports must be at least 1000, depending on the amount used. Ports should not be within the ephemeral ports range, nor in use by other running software. |
| ENABLE_EPM | If true, EPM Shared Services identity provider is used | false | If false, WebLogic security (identity provider) is used |
| EPM_ORACLE_HOME | Full path to folder of EPM Oracle Home | - | Use this variable if ENABLE_EPM is true. |

**Table 4-1 (Cont.) Response File Variables**

| Variable Name | Description | Default Value | Notes |
|---|---|---|---|
| EPM_ORACLE_INSTANCE | Full path to folder of EPM Oracle Instance | - | Use this variable if ENABLE_EPM is true. |
| ENABLE_WINDOWS_SERVICE | True if Essbase Windows Services enabled. | - | If true, enable Essbase Windows Services. |
| EPM_ORACLE_CLUSTER_NAME | Name for Essbase cluster in EPM Oracle instance | - | Name to be register Essbase Instance in EPM Shared Services |

### Sample Response File

The following is a sample configuration response file. On your server, a response file is generated in /tmp each time you run the Configuration Tool, reflecting your configuration choices. Lines beginning with # are comments, for descriptive purposes only. The uncommented lines reflect (and cause) actual configuration changes. If you want to use this sample response file as a template when running configuration, first update the uncommented lines to reflect your choices of variables and values to use.

```
##############################################################################
##                                                                          ##
## Copyright (c) 1996, 2021 Oracle. All rights reserved.                    ##
##                                                                          ##
## Specify values for the variables listed below to customize               ##
## your configuration.                                                      ##
##                                                                          ##
## Specify values in the following format:                                  ##
##                                                                          ##
##         Type         Example                                             ##
##         ----         -------                                             ##
##         string       Sample Value                                        ##
##         boolean      TRUE or FALSE                                       ##
##         number       1000                                                ##
##                                                                          ##
##############################################################################
##############################################################################

#------------------------------------------------------------------------#
# Name        : DOMAIN_NAME
# Type        : string
# Description : Domain name.
#------------------------------------------------------------------------#
DOMAIN_NAME=essbase_domain

#------------------------------------------------------------------------#
# Name        : DOMAIN_ROOT
# Type        : string
# Description : Domains location.
#------------------------------------------------------------------------#
DOMAIN_ROOT=c\:\\TEST\\12esscs\\dist\\user_projects\\domains

#------------------------------------------------------------------------#
```

```
# Name        : ARBORPATH
# Type        : string
# Description : Essbase application path.
#-------------------------------------------------------------------#
ARBORPATH=c\:\\TEST\\12esscs\\dist\\user_projects\\applications\\essbase

#-------------------------------------------------------------------#
# Name        : ADMIN_USERNAME
# Type        : string
# Description : Admin username of WebLogic.
#-------------------------------------------------------------------#
ADMIN_USERNAME=weblogic

#-------------------------------------------------------------------#
# Name        : DATABASE_TYPE
# Type        : string
# Description : Type of the database connection.
#-------------------------------------------------------------------#
DATABASE_TYPE=DB_SQLSERVER

#-------------------------------------------------------------------#
# Name        : DATABASE_CONNECT_STRING
# Type        : string
# Description : Connection string. Oracle connection string: host:port:sid,
host:port/service_name, or (description...). MS SQL Server connection string:
host:port:database
#-------------------------------------------------------------------#
DATABASE_CONNECT_STRING=testdb.uu.oracle.com\:1433\:user

#-------------------------------------------------------------------#
# Name        : CREATE_DATABASE_SCHEMA
# Type        : string
# Description : Essbase RDBMS Schemas. Available values CREATE and
USE_EXISTING
#-------------------------------------------------------------------#
CREATE_DATABASE_SCHEMA=USE_EXISTING

#-------------------------------------------------------------------#
# Name        : DATABASE_PREFIX
# Type        : string
# Description : Prefix for DB schemas.The prefix name must be a minimum of
one character in length and cannot exceed 12 alphanumeric characters in
length. Prefix should not start with a number.
#-------------------------------------------------------------------#
DATABASE_PREFIX=test_prefix

#-------------------------------------------------------------------#
# Name        : SECURE_MODE
# Type        : boolean
# Description : True if use secure connection.
#-------------------------------------------------------------------#
SECURE_MODE=false

#-------------------------------------------------------------------#
# Name        : MACHINE_NAME
# Type        : string
```

```
# Description : WebLogic Machine Name.
#--------------------------------------------------------------------#
MACHINE_NAME=m1

#--------------------------------------------------------------------#
# Name        : NODE_MANAGER_PORT
# Type        : number
# Description : Port of the WebLogic Node Manager. Default value is 9556.
#--------------------------------------------------------------------#
NODE_MANAGER_PORT=9556

#--------------------------------------------------------------------#
# Name        : NODE_MANAGER_LISTEN_ADDRESS
# Type        : string
# Description : Listen Address of WebLogic Node Manager. Default value is
fully qualified domain name.
#--------------------------------------------------------------------#
NODE_MANAGER_LISTEN_ADDRESS=abc.bac.com

#--------------------------------------------------------------------#
# Name        : ADMIN_SERVER_PORT
# Type        : number
# Description : Port of the Admin Server. Default value is 7001.
#--------------------------------------------------------------------#
ADMIN_SERVER_PORT=7001

#--------------------------------------------------------------------#
# Name        : ADMIN_SERVER_SSL_PORT
# Type        : number
# Description : Secure Port of the Admin Server. Default value is 7002.
#--------------------------------------------------------------------#
ADMIN_SERVER_SSL_PORT=7002

#--------------------------------------------------------------------#
# Name        : ADMIN_SERVER_LISTEN_ADDRESS
# Type        : string
# Description : Listen Address of Admin Server. Empty string means "All local
addresses".
#--------------------------------------------------------------------#
ADMIN_SERVER_LISTEN_ADDRESS=All Local Addresses

#--------------------------------------------------------------------#
# Name        : MANAGED_SERVER_PORT
# Type        : number
# Description : Port of the Managed Server. Default value is 9000.
#--------------------------------------------------------------------#
MANAGED_SERVER_PORT=9000

#--------------------------------------------------------------------#
# Name        : MANAGED_SERVER_SSL_PORT
# Type        : number
# Description : Secure Port of the Managed Server. Default value is 9001.
#--------------------------------------------------------------------#
MANAGED_SERVER_SSL_PORT=9001

#--------------------------------------------------------------------#
```

```
# Name        : MANAGED_SERVER_LISTEN_ADDRESS
# Type        : string
# Description : Listen Address of Managed Server. Empty string means "All
local addresses".
#-------------------------------------------------------------------#
MANAGED_SERVER_LISTEN_ADDRESS=All Local Addresses

#-------------------------------------------------------------------#
# Name        : ENABLE_EAS
# Type        : boolean
# Description : True if use Essbase Administration Console Server.
#-------------------------------------------------------------------#
ENABLE_EAS=false

#-------------------------------------------------------------------#
# Name        : AGENT_PORT
# Type        : number
# Description : Port of the JAgent.  Default value is 1423.
#-------------------------------------------------------------------#
AGENT_PORT=1423

#-------------------------------------------------------------------#
# Name        : AGENT_SSL_PORT
# Type        : number
# Description : Secure Port of the JAgent. Default value is 6423.
#-------------------------------------------------------------------#
AGENT_SSL_PORT=6423

#-------------------------------------------------------------------#
# Name        : ESSBASE_SERVER_MIN_PORT
# Type        : number
# Description : Minimal Port of the Essbase Server connection.  Default value
is 30768.
#-------------------------------------------------------------------#
ESSBASE_SERVER_MIN_PORT=30768

#-------------------------------------------------------------------#
# Name        : ESSBASE_SERVER_MAX_PORT
# Type        : number
# Description : Maximal Port of the Essbase Server connection.  Default value
is 31768.
#-------------------------------------------------------------------#
ESSBASE_SERVER_MAX_PORT=31768

#-------------------------------------------------------------------#
# Name        : ENABLE_EPM
# Type        : boolean
# Description : True if EPM Shared Services Identity provider enabled.
#-------------------------------------------------------------------#
ENABLE_EPM=true

#-------------------------------------------------------------------#
# Name        : EPM_ORACLE_HOME
# Type        : string
# Description : Path to the folder of EPM Oracle Home.
#-------------------------------------------------------------------#
```

```
EPM_ORACLE_HOME=\\\\abc.uu.oracle.com\\C$\\Oracle\\Middleware\\EPMSystem11R1

#-------------------------------------------------------------------#
# Name        : EPM_ORACLE_INSTANCE
# Type        : string
# Description : Path to the folder of EPM Oracle Instance.
#-------------------------------------------------------------------#
EPM_ORACLE_INSTANCE=\\\\abc.uu.oracle.com\\C\\Oracle\\Middleware\
\user_projects\\epmsystem1

#-------------------------------------------------------------------#
# Name        : ENABLE_WINDOWS_SERVICE
# Type        : boolean
# Description : True if Essbase Windows Services enabled.
#-------------------------------------------------------------------#
ENABLE_WINDOWS_SERVICE=false

#-------------------------------------------------------------------#
# Name        : EPM_ORACLE_CLUSTER_NAME
# Type        : string
# Description : Unique name for Essbase Cluster Name in EPM Oracle Instance.
#-------------------------------------------------------------------#
EPM_ORACLE_CLUSTER_NAME=ESSBASE FINANCIAL SERVICE
```

# Delete RCU Schemas for Essbase

To delete or clean up your Essbase schemas, use the Fusion Middleware RCU utility and the following steps, with the Drop Repository option. If you prefer to use the command-line method with Silent mode, skip to that section near the end of this topic.

### Drop Schemas using the Utility

1. In the Oracle Home where Fusion Middleware is installed, open a terminal in `/oracle_common/bin`. For example, open a terminal in `/scratch/user/oracle_home/oracle_common/bin`.
2. Run the `rcu` command to launch the Repository Creation Utility.

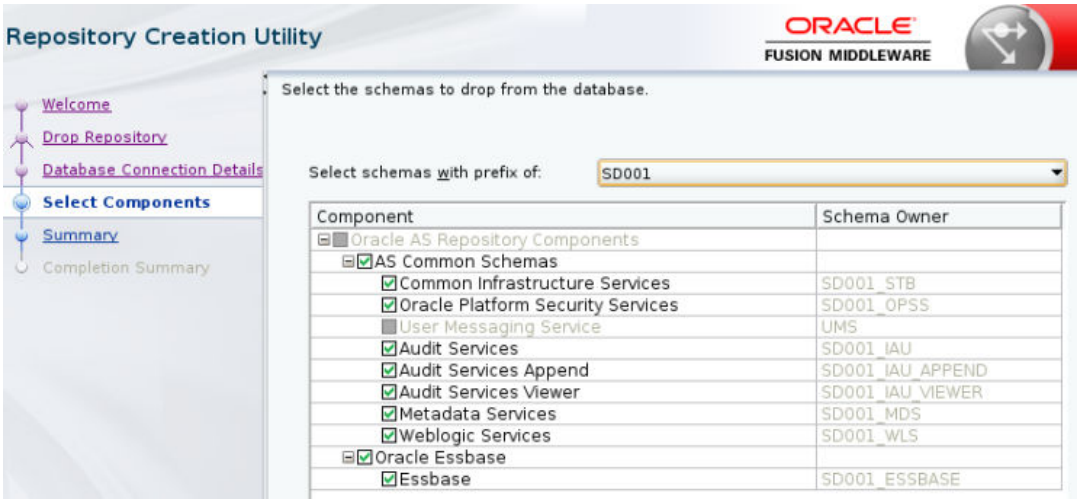
   Linux Example

   ```
   ./rcu
   ```

   Windows Example

   ```
   rcu.bat
   ```

3. On the Welcome page, click **Next**.
4. On the Create Repository page, click **Drop Repository**, and then **Next**.
5. On the Database Connection Details page, enter the connection details, and click **Next**.
6. On the Select Components page, be very careful to select the correct schema prefix for the schemas that you want to delete.




Click **Next**, and **OK** to confirm.

7. On the Summary page, it's recommended to click **Save Response File**, if you might want to do a silent schema removal later. Review the summary of schemas to be dropped, and click **Drop** to remove them.
8. Review the Completion Summary page, and click **Close**.

### Drop Schemas using Silent mode

For the Silent mode to drop all RCU schemas, prefixes, and components, you can use the command syntax below. The *connectString* can be found in the configuration log, rcu log, or response file generated during configuration. If the RCU is connected via SQL tools (such as SQL Developer or SQL Plus), close all active connections before proceeding to drop RCU schemas.

```
<ORACLE_HOME>/oracle_common/bin/rcu -silent -dropRepository -databaseType
oracle
      -connectString myhost.example.com:1521/orcl -dbUser sys -dbRole sysdba -
schemaPrefix
      ABC123 -component MDS -component WLS -component OPSS -component STB -
component IAU -component IAU_APPEND
      -component IAU_VIEWER -component ESSBASE -f
```

If you're not aware of RCU components to provide as arguments, use the following syntax to list them.

```
ORACLE_HOME/oracle_common/bin/rcu -silent -listComponents
```

## Essbase Server Configuration File (essbase.cfg)

In addition to using the Configuration Tool and the Silent mode configuration option, you can change Essbase server configuration as needed by editing a file.

The server configuration file, `essbase.cfg` is located in `<Domain Root>/<Domain Name>/config/fmwconfig/essconfig/essbase`. When you run Configuration Tool, it writes the following configuration properties to `essbase.cfg`:

- AGENTPORT—Clear port reserved for Essbase Agent

- AGENTSECUREPORT—Secure port reserved for Essbase Agent
- ENABLESECUREMODE—**true** if you enable secure connection mode with Transport Layer Security (TLS)
- ENABLECLEARMODE—**true** if you did not enable secure connection mode with Transport Layer Security (TLS)
- CLIENTPREFERREDMODE—**secure** or **clear** indicating the connection security used for communication with Essbase client tools
- SERVERPORTBEGIN—Starting port number of a range of ports reserved for Essbase application server processes
- SERVERPORTEND—Ending port number of a range of ports reserved for Essbase application server processes
- AUTHENTICATIONMODULE—Mode selected for Essbase user and group authentication
- ASODEFAULTCACHESIZE—Default size for the aggregate storage cache associated with aggregate storage cubes

You can edit `essbase.cfg` as needed. To learn how, see Set Server-Level Configuration Properties in *Configuration Reference for Oracle Essbase* documentation.

## Configure a Load Balancer to Support Failover

If you plan to install and configure more than one Essbase instance, to support failover, you need a front-end load balancer.

One option to consider for a load balancer is Oracle HTTP Server, because it is integrated with WebLogic and provides web services for Oracle Fusion Middleware.

Another option is Apache HTTPD Server.

> **Note:**
>
> If you're connecting through Smart View, using the URL `/aps/SmartView`, you need to change the URL. See Redirect to New Essbase Smart View Connection URL. Alternatively, you can configure redirection to the new URL on the web server. If you're using Oracle HTTP Server (OHS) or Apache HTTPD Server, redirect the URL while modifying the Oracle HTTP Server configuration, as described in this topic.

**Oracle HTTP Server or Apache HTTPD Server**

1. First, Install and Configure Oracle HTTP Server or Apache HTTPD Server.
2. Then, locate the file `mod_wl_ohs.conf` under your OHS domain root in the Oracle HTTP Server installation.
   Example:

   `<OHS>/oracle/user_projects/domains/SOHSDomain/config/fmwconfig/components/OHS/ohs1/mod_wl_ohs.conf`

   (where OHS is the home location of the Oracle HTTP Server installation).

3. Insert the appropriate “weblogic_module” entries to `mod_wl_ohs.conf`. You don’t need to include `eas` and `easconsole` location entries unless you configured Essbase to use Essbase Administration Services on Host 1..

```
<IfModule weblogic_module>
ConnectTimeoutSecs 10
ConnectRetrySecs 2
DebugConfigInfo ON
WLSocketTimeoutSecs 2
WLIOTimeoutSecs 300
Idempotent ON
FileCaching ON
KeepAliveSecs 20
KeepAliveEnabled ON
DynamicServerList ON
WLProxySSL OFF
</IfModule>
<Location /essbase>
SetHandler weblogic-handler
WebLogicCluster hostname:managed_server_port
Debug ALL
KeepAliveSecs 20
KeepAliveEnabled ON
DebugConfigInfo ON
</Location>

<Location /eas>
SetHandler weblogic-handler
WebLogicCluster hostname:eas_managed_server_port
Debug ALL
KeepAliveSecs 20
KeepAliveEnabled ON
DebugConfigInfo ON
</Location>

<Location /easconsole>
SetHandler weblogic-handler
WebLogicCluster hostname:eas_managed_server_port
Debug ALL
KeepAliveSecs 20
KeepAliveEnabled ON
DebugConfigInfo ON
</Location>
```

4. Edit the text you inserted into `mod_wl_ohs.conf` as follows:

   a. Edit `<Location /Essbase>` and replace `hostname` with the host name of Host 1 and `managed_server_port` with the Essbase WebLogic managed server port of Host 1. Using a comma separated format, add each additional Essbase managed server node that you plan to include in your cluster.
   Example:

   Let's say Essbase Host 1 runs on `hostname1:managed_server_port1` and Host 2 runs on `hostname2:managed_server_port2`.

To specify the servers in comma separated format, type (with no spaces added):

```
hostname1:managed_server_port1,hostname2:managed_server_port2
```

Do not add the prefix http or https to any host name.

b. Edit `<Location /eas>` and replace `hostname` with the host name of Host 1 and `eas_managed_server_port` with the Essbase Administration Services WebLogic managed server port of Host 1.

c. Edit `<Location /easconsole>` and replace `hostname` with the host name of Host 1 and `eas_managed_server_port` with the Essbase Administration Services WebLogic managed server port of Host 1.

5. Save the configuration.

6. Restart Oracle HTTP Server.

   a. To stop Oracle HTTP Server:

      i. Navigate to the `bin` directory under your OHS domain root.

      ```
      cd ./user_projects/domains/SOHSDomain/bin/
      ```

      ii. Run the script to stop the OHS server component.

      ```
      ./stopComponent.sh ohs1
      ```

      iii. In the background, run the script to stop the Node Manager.

      ```
      nohup ./stopNodeManager.sh &
      ```

      iv. At the password prompt, enter the password that was entered during the installation.

   b. To start Oracle HTTP Server:

      i. Navigate to the bin directory under your OHS domain root.

      ```
      cd ./user_projects/domains/SOHSDomain/bin/
      ```

      ii. In the background, run the script to start the Node Manager.

      ```
      nohup ./startNodeManager.sh &
      ```

      iii. Run the script to start the OHS server component.

      ```
      ./startComponent.sh ohs1
      ```

      iv. At the password prompt, enter the password that was entered during the installation.

   For Oracle HTTP Server SSL configuration, see Configure mod_wl_ohs.

**Sample Code for SSL Offload using Apache HTTPD Server**

Here is a sample HTTP configuration of SSL offload using Apache HTTPD Server, using SSL default port 443 (or any other selected port) for HTTPS offload redirect to Essbase.

```
#
# Macro file for the Essbase proxy settings
#

<Macro EssbaseProxy $TargetUrl>
ProxyPreserveHost On
```

```
ProxyPassReverse  / $TargetUrl/
ProxyErrorOverride Off

RewriteEngine On
RewriteCond %{HTTP:X-Forwarded-Proto} ^.+$ [NC]
RewriteRule ^/$
%{HTTP:X-Forwarded-Proto}://%{HTTP_HOST}/essbase/jet/ [L,R]
RewriteCond %{HTTPS} on
RewriteRule ^/$                       https://%{HTTP_HOST}/essbase/jet/
[L,R]RewriteRule ^/$                       http://%{HTTP_HOST}/essbase/jet/
[L,R]

RewriteCond %{HTTP:X-Forwarded-Proto} ^.+$ [NC]
RewriteRule ^/essbase(/)?$
%{HTTP:X-Forwarded-Proto}://%{HTTP_HOST}/essbase/jet/ [L,R]
RewriteCond %{HTTPS} on
RewriteRule ^/essbase(/)?$            https://%{HTTP_HOST}/essbase/jet/
[L,R]RewriteRule ^/essbase(/)?$            http://%{HTTP_HOST}/essbase/jet/
[L,R]

# jsession redirect issue
RewriteCond %{HTTP:X-Forwarded-Proto} ^.+$ [NC]
RewriteRule ^/essbase/jet(;.*)?$
%{HTTP:X-Forwarded-Proto}://%{HTTP_HOST}/essbase/jet/ [L,R]
RewriteCond %{HTTPS} on
RewriteRule ^/essbase/jet(;.*)?$      https://%{HTTP_HOST}/essbase/jet/
[L,R]RewriteRule ^/essbase/jet(;.*)?$      http://%{HTTP_HOST}/essbase/jet/
[L,R]

# Logout url
RewriteCond %{HTTP:X-Forwarded-Proto} ^.+$ [NC]
RewriteRule ^/essbase/jet/logout.html
%{HTTP:X-Forwarded-Proto}://%{HTTP_HOST}/essbase/jet/ [L,R]
RewriteCond %{HTTPS} on
RewriteRule ^/essbase/jet/logout.html https://%{HTTP_HOST}/essbase/jet/
[L,R]RewriteRule ^/essbase/jet/logout.html http://%{HTTP_HOST}/essbase/jet/
[L,R]

# Support redirect_uri logout for virtual hosts
RewriteCond %{QUERY_STRING} ^logout=$
RewriteCond %{HTTP:X-Forwarded-Proto} ^.+$ [NC]
RewriteRule ^/essbase/redirect_uri$
%{HTTP:X-Forwarded-Proto}://%{HTTP_HOST}/essbase/redirect_uri?logout=%{HTTP:X-
Forwarded-Proto}://%{HTTP:X-Forwarded-Host}/essbase/jet/logout.html [L,R]
RewriteCond %{QUERY_STRING} ^logout=$
RewriteCond %{HTTPS} on
RewriteRule ^/essbase/redirect_uri$
https://%{HTTP_HOST}/essbase/redirect_uri?logout=https://%{HTTP_HOST}/
essbase/jet/logout.html [L,R]
RewriteCond %{QUERY_STRING} ^logout=$
RewriteRule ^/essbase/redirect_uri$
http://%{HTTP_HOST}/essbase/redirect_uri?logout=http://%{HTTP_HOST}/
essbase/jet/logout.html [L,R]

# Set weblogic specific headers
<If "%{HTTP:X-Forwarded-Proto} == 'https' || %{HTTPS} == 'on'">
```

```
  RequestHeader set WL-Proxy-SSL "true"
  RequestHeader set IS_SSL       "ssl"
</If>

<Location "/">
   Options -Indexes
   SetOutputFilter DEFLATE
   SetEnvIfNoCase Request_URI \.(?:gif|jpe?g|png)$ no-gzip dont-vary
</Location>

<Location "/essbase">
   ProxyPass "$TargetUrl/essbase"
</Location>

<Location "/essbase/redirect_uri">
   ProxyPass "!"
</Location>

<Location "/weblogic/ready">
   ProxyPass "$TargetUrl/weblogic/ready"
</Location>

</Macro>
```

# Modify CRASHDUMP Configuration

By default, CRASHDUMP configuration is set to automatically clear created Essbase Application Folders stored in the tmp folder. You must delete the core files in this location, as necessary.

After Essbase configuration, check your CRASHDUMP and CRASHDUMPLOCATION settings in the Essbase configuration file - you may need to change the default location setting to your specified location.

- CRASHDUMP—indicates whether Essbase saves a core dump to a file when an abnormal termination of an application server process occurs.
- CRASHDUMPLOCATION—specifies the location where Essbase saves a core dump file when an abnormal application termination occurs. By default, CRASHDUMPLOCATION configuration is set to the tmp folder.

For more information on essbase.cfg, see Essbase Server Configuration File (essbase.cfg). To edit `essbase.cfg` as needed, see Set Server-Level Configuration Properties in *Configuration Reference for Oracle Essbase* documentation.

# Redirect to New Essbase Smart View Connection URL

If you're using Smart View, you need to modify your connection URL.

If you're connecting through Smart View, using the URL `/aps/SmartView`, it's now required to be changed to `/essbase/smartview`. Alternatively, you can configure redirection to the new URL on the web server.

If you're using Oracle HTTP Server (OHS) or HTTPD Server, you can configure and map your Oracle HTTP Server to redirect your connection to `/essbase/smartview`. First, install Oracle HTTP Server if it isn't already installed. Then, modify its configuration file to allow users to

redirect to the new URL. Follow the steps in Configure a Load Balancer to Support Failover and insert the following rule in the configuration file:

```
RewriteRule ^/aps/SmartView /essbase/smartview [PT,L]
```

Alternatively, to redirect all APS URLs, use the following rule:

```
RewriteRule ^/aps/(.*)$ /essbase/$1 [PT,L]
```

# Expand Limit for SQL IN Clauses in Drill Through Reports

Resolve a drill through reports error by increasing the SQL IN clause limit beyond the default of 1000 members.

If drill through reports fail with error

```
'ERROR: relation <member name> does not exist'
```

The failure occurs because SQL IN clauses are limited to 1000 members by default. This default exists for Essbase and for Oracle Database.

> **Caution:**
>
> The Essbase platform includes scripts in `<DOMAIN HOME>/bin` that can customize the environment and behaviors of Essbase functionality. However, making changes to these domain environment or startup scripts can have unintended effects, including startup failure. Oracle recommends making changes in a test environment first. Before editing these scripts, always:
>
> 1. Stop the Essbase managed servers, using `<DOMAIN HOME>/esstools/bin/stop.sh` (on Linux), or `<DOMAIN HOME>\esstools\bin\stop.cmd`(on Windows).
> 2. In `<DOMAIN HOME>/bin`, make a backup copy of the file you want to edit. For example,
>
>    On Linux
>
>    ```
>    cp setStartupEnv.sh setStartupEnv_bak.sh
>    ```
>
>    On Windows
>
>    ```
>    copy setStartupEnv.cmd setStartupEnv_bak.cmd
>    ```
>
> 3. Edit carefully, using only Oracle's documented instructions, or working with Oracle Support.
> 4. Restart Essbase, using `<DOMAIN HOME>/esstools/bin/start.sh` (on Linux), or `<DOMAIN HOME>\esstools\bin\start.cmd`(on Windows). Check that startup completed normally.

To increase the SQL IN clause limit for drill through, if expanded limits are supported by your external database,

1. Stop the Essbase services (see Stop, Start, and Check Servers).
2. On the machine where Essbase is deployed, navigate to `<Domain Home>/bin` (see Environment Locations in the Essbase Platform).
3. Make a backup copy of the startup script, `setStartupEnv.sh` (Linux) or `setStartupEnv.bat` (Windows). Save it with a different name; for example: `cp setStartupEnv.sh setStartupEnv_orig.sh`
4. Open `setStartupEnv.sh` or `setStartupEnv.bat` for editing.
5. Add the configuration lines to increase the limit beyond 1000.
   Linux Example (setStartupEnv.sh):

   ```
   JAVA_OPTIONS="${JAVA_OPTIONS} -Ddtr.in.clause.limit=15000" export
   JAVA_OPTIONS
   ```

   Windows Example (setStartupEnv.bat):

   ```
   set JAVA_OPTIONS=%JAVA_OPTIONS% "-Ddtr.in.clause.limit=15000"
   ```

6. Save `setStartupEnv.sh` or `setStartupEnv.bat`.
7. Start the Essbase services (see Stop, Start, and Check Servers).

## Configure Essbase Servers in a Failover Cluster

Active-passive failover solutions are common in Essbase 11g On-Premise deployments. Users migrating to Essbase 21c can also implement active-passive failover clusters for Essbase Agent using WebLogic and a load balancer.

When configuring Essbase failover, the goal is to:

- Set up failover mode (or active-passive mode) for the Essbase Agent.
- Set up active-active mode for Essbase web interface, REST endpoints and Provider Services. These always connect to the single active Essbase node.

An active-passive Essbase cluster consists of two or more Essbase instances, one on each node, that share a common storage for configuration and data. Storage is shared across two or more servers (for example, using a SAN), removing the need for the administrator to synchronize storage, as well as the constraint of read-only support. Essbase uses database tables to ensure that only one agent and its associated servers are active, to avoid data corruption on writes. During installation and configuration, a table is created to hold information on configuration and application data in the cluster.

Compared to Essbase 11g On-Premise, where Essbase failover is managed by an external agent (OPMN), in Essbase 21c, the WebLogic architecture supports Essbase failover with a central request leasing system. The Essbase instance that acquires the lease becomes the active node. Other nodes are waiting in a loop, trying to acquire the lease.

| Installation Type | Component | Essbase 11.1.2.4 | Essbase 21c |
|---|---|---|---|
| Single Node | Provider Services | • Provider Services runs on a single managed server, which is always active.<br>• If a failure occurs, WebLogic Node Manager restarts the managed server. | Same as 11.1.2.4 |
| - | Essbase Agent | • Single instance of the Essbase Agent process.<br>• If a failure occurs, OPMN restarts the agent instance on the same node. | • Essbase Java Agent runs on a single managed server, which is considered the active node.<br>• If the managed server fails, Node Manager restarts the managed server. |
| - | Essbase application server. | If the Essbase application server fails, the Essbase agent restarts it on the next server request. | Same as 11.1.2.4. |
| Multi-Node (Active/ Passive) | Provider Services | • Provider Services is deployed with each node in the cluster.<br>• All the managed servers are up and running at the same time.<br>• Provider Services cannot share sessions across the nodes. | Same as 11.1.2.4. |

| Installation Type | Component | Essbase 11.1.2.4 | Essbase 21c |
|---|---|---|---|
| - | Essbase Agent | • Only failover support; no load balancing support for Essbase.<br>• Essbase lifecycle is managed by OPMN.<br>• OPMN-managed active-passive solution.<br>• Shared ARBORPATH (NFS) or Block storage mounted/ unmounted by OPMN.<br>• Whenever Essbase running in the active node is not reachable (OPMNPing), OPMN restarts Essbase on a different node.<br>• The newly launchedEssbase instance updates the lease tables with its host details.<br>• Existing Essbase applications, which were running in the previous node are unloaded. Until the unload process is complete, the agent in the new node is not able to launch those applications.<br>• As a new ESSBASE process is started on a different node, downtime could be several seconds after AGENTLEASEEXPIRATIONTIME seconds.<br>• OPMN runs the block storage unmount command on the previous active node (If the node is alive) and the mount command on the current active node. | • Only failover support; no load balancing support for Essbase.<br>• Essbase life cycle is managed by WebLogic, and Node Manager manages all the WebLogic instances.<br>• Self-managed active-passive solution.<br>• Shared Essbase Applications Directory (formerly ARBORPATH) (NFS) + Shared Relational Database for Shared Essbase.<br>• Essbase Java Agent is deployed in the same managed server as Provider Services in all the active nodes. Essbase Java Agent instances use a leasing algorithm to ensure only one node runs at any point in time. Although Essbase Java Agent is up and running in all the nodes, only one of them is available for servicing. The rest of the Essbase Java Agent instances remain in standby mode, and are not listening for any Essbase requests.<br>• Whenever the active node is unable to renew the lease, another Essbase Java Agent instance from a passive node gets activated.<br>• Newly launched Essbase updates the lease tables with its host details. |

| Installation Type | Component | Essbase 11.1.2.4 | Essbase 21c |
|---|---|---|---|
| | | | • Existing Essbase applications, which were running in the previous node are unloaded. Until the unload process is complete, the agent in the new node is not available for service.<br>• When there is a failover, the new Essbase Java Agent instance immediately takes over after AGENTLEASEEXPIRATIONTIME seconds.<br>• Essbase Java Agent (within WebLogic) runs the block storage unmount command on the previous active node (If the node is alive and it was a graceful lease release) and the mount command on the current active node. |
| - | Essbase Application Server | • Restarted in the same system whenever there is a failure.<br>• When the Essbase Agent fails or is stopped, servers are shut down. Until the shutdown is complete, the same applications cannot be launched in the new active node.<br>• Essbase server processes use lease tables. | Same as 11.1.2.4, except for server-level leasing. |

## Essbase Failover Prerequisites

At least two Essbase server machines (hosts) are required for a failover setup. Although more than two hosts can be established, in this documentation we will refer to Host 1 and Host 2.

Host 1 will be the primary node and will have all services not clustered (such as AdminServer and optionally EAS Lite). Host 2 will be the secondary node and will only run Essbase.

1. Create a directory in a shared network drive that is accessible to both the nodes for storing the Essbase `<Applications Directory>`. If you do not know where `<Application Directory>` is, see Environment Locations in the Essbase Platform for details. This directory will be used when Essbase is configured on Host 1. The mounted path should be the same on both the hosts.
   For example, if `/nfs/essbase_data` is mounted on `/u01/essbase_data` in Host 1, then it should be mounted in the same path, `/u01/essbase_data` in Host 2 as well.

   > **Note:**
   >
   > Universal/Uniform Naming Convention (UNC) paths are not supported on Windows for the `<Application Directory>` in a failover setup.

2. Install Essbase on every node.
   - Each node in the cluster must have the same `<ORACLE_HOME>` directory path; but this path should not be a shared directory.
   - The installation Operating System user name should be the same on each node.
   - Each node should have its own oraInventory.
3. Configure Essbase, only on Host 1.
   - **Important**: during the configuration on Host 1, specify the shared directory (created in step 2) as the `<Application Directory>`.
   - Record the following information during Host 1 configuration:
     - Domain Location
     - Domain Name
     - NodeManager port
     - AdminServer port
     - Managed Server port
   - **Important**: do not configure Essbase on Host 2. By default, the installation takes you next to the Essbase configuration screen. Cancel and exit the tool for Host 2.
4. Install an http server or load balancer for managing the nodes. In this topic, we will assume it is running on Host 1, although it must only be available via the network to the two hosts. If you don't have an http server or load balancer, you can follow steps to Install Oracle HTTP Server (OHS) and Configure Oracle HTTP Server.
5. If the primary node is enabled for TLS (SSL), then complete the TLS configuration on the primary node before configuring the failover node.
   a. Set up Weblogic TLS Connection for Essbase.

      ```
      java -cp $ORACLE_HOME/essbase/lib/essbaseconfig.jar
      com.oracle.wizard.operation.helper.ssl.SslConfigHelper
      [RESPONSE_FILE=<response file> | DOMAIN_HOME=<${DOMAIN_HOME}>]
      ```

   b. Configure TLS for Essbase failover using the TLS Configuration Utility.
      The SAN property in `tls_tools.properties` should have OHS, primary node, and failover node IP address and DNS entries.

Example:

```
SAN=IP:10.x.x.11,IP:10.x.x.13,IP:10.x.x.17,DNS:myhost,DNS:myhost.example
.com
certCA=
certFile=
```

c. In EPM deployments only, EPM WebLogic Server should be stopped before failover configuration and started after failover configuration.

> **Note:**
>
> If you plan to set up a failover environment, and you are using EPM Shared Services for authentication, then you must install EPM 11g Services to a shared network location accessible by all the Essbase nodes. If this is not possible, you can install only the EPM Foundation component locally in each Essbase node, but pointing to the same EPM Schema. Each Essbase node must be able to find the EPM_ORACLE_HOME and EPM_ORACLE_INSTANCE locations associated with your EPM installation.

## Set up an Essbase Failover Environment Using the Failover Setup Script

Starting with Release 21.5.2, you can use the Essbase Failover Setup Script to automate the following workflows which, in previous releases, were required to be done manually:

- Manual Steps for Essbase Failover Configuration on the Primary Node (Host 1)
- Manual Steps for Failover Configuration on the Secondary Node (Host 2)

Instead of following manual steps, use the following workflow to automate failover setup in Release 21.5.2 and higher.

### Get Started

1. Follow the steps in Essbase Failover Prerequisites.
2. Log in to the primary node, open a command prompt or terminal, and ping the secondary (failover) node. Make note of its public IP.
   Example

   ```
   ping secondaryhost.example.com
   ```

3. Log in to the secondary (failover) node, open a command prompt or terminal, and ping the primary node. Make note of its public IP.
   Example

   ```
   ping primaryhost.example.com
   ```

### Set Up the Primary Node (Host 1)

1. On the primary node (host 1), open the Essbase Server configuration file, and add the configuration property: FAILOVERMODE TRUE. See Set Server-Level Configuration Properties.

2. On the primary node (host 1), navigate to the Essbase Failover Setup Script in `<Essbase Product Home>/modules/oracle.essbase.sysman/scripts/failover`.
If you do not know where `<Essbase Product Home>` is, see Environment Locations in the Essbase Platform for details.

   Linux Example

   ```
   cd /scratch/username/oracle_home/essbase/modules/oracle.essbase.sysman/
   scripts/failover
   ```

   Windows Example

   ```
   chdir
   C:\Oracle\Middleware\Oracle_Home\essbase\modules\oracle.essbase.sysman\scri
   pts\failover
   ```

3. Required for Linux only: On the primary node (host 1), change the access permissions to make the Essbase Failover Setup Script executable.
Example

   ```
   chmod +x essbaseFailoverSetup.sh
   ```

4. On the primary node (host 1), run the Essbase Failover Setup Script to set up the primary configuration. The script usage syntax is as follows:

   ```
   essbaseFailoverSetup.sh [-primaryconfig] [-failoverconfig] [-listnodes] [-
   deletenode]
   -primaryconfig  - For  primary node configuration
   -failoverconfig - For failover node configuration
   -listnodes - For listing failover nodes
   -deletenode - For removing the failover node from the cluster
   ```

   Script Session Example

   a. Run the script with the `-primaryconfig` option.
   Linux Example

      ```
      ./essbaseFailoverSetup.sh -primaryconfig
      ```

      Windows Example

      ```
      .\essbaseFailoverSetup.cmd -primaryconfig
      ```

   b. If there are multiple domains configured in the WebLogic system, the script will display all the domain homes, and you are prompted to choose the domain home. If there is a single domain home, then the system uses that domain without a prompt.

      Example:

      ```
      Identified multiple domains, listed as below:
      Choose the Essbase domain home path(<DOMAIN_HOME>) from the list:
      ../domains/esscs
      ../domains/esscs2
      ```

At the prompt, enter the shared network path for the Essbase `<Application Directory>`. It must be the same network path entered in step 1 of Essbase Failover Prerequisites.

Linux Example

```
/u01/essbase_data
```

Windows Example

```
z:\essbase_mount
```

> **Note:**
>
> In an environment set up for failover, the application directory must be a shared network mount accessible by both hosts.

c. At the prompt, enter the failover node's name. If TLS was enabled, enter the Managed Server Secure Port. If TLS was not enabled, enter the Managed Server port. Enter the Node Manager port.

Examples

```
essbase_domain2
9001
9555
```

If you entered a secure port, you must also complete the configuration of TLS for Essbase failover.

d. At the prompts, enter the failover and primary nodes' public IP addresses that you obtained in previous steps.
Examples

```
100.x.x.01
100.x.x.02
```

Once you have provided all the inputs to the script, it finishes configuring failover for the primary node. Now you can move on to secondary node configuration.

**Set up the Secondary Node (Host 2)**

1. SSH to the secondary node, Host 2.
2. Navigate to the Essbase Failover Setup Script in `<Essbase Product Home>/modules/oracle.essbase.sysman/scripts/failover`.
If you do not know where `<Essbase Product Home>` is, see Environment Locations in the Essbase Platform for details.

Linux Example

```
cd /scratch/username/oracle_home/essbase/modules/oracle.essbase.sysman/
scripts/failover
```

Windows Example

```
chdir
C:\Oracle\Middleware\Oracle_Home\essbase\modules\oracle.essbase.sysman\scri
pts\failover
```

3. Required for Linux only: On the secondary/failover node (host 2), change the access permissions to make the Essbase Failover Setup Script executable.
Example

```
chmod +x essbaseFailoverSetup.sh
```

4. On the secondary/failover node (host 2), run the Essbase Failover Setup Script to set up the failover node configuration.
The script usage syntax is as follows:

```
essbaseFailoverSetup.sh [-primaryconfig] [-failoverconfig] [-listnodes] [-
deletenode]
-primaryconfig  - For  primary node configuration
-failoverconfig - For failover node configuration
-listnodes - For listing failover nodes
-deletenode - For removing the failover node from the cluster
```

Script Session Example

a. Run the script with the `-failoverconfig` option.
Linux Example

```
./essbaseFailoverSetup.sh -failoverconfig
```

Windows Example

```
.\essbaseFailoverSetup.cmd -failoverconfig
```

b. At the prompt, enter the shared network path for the Essbase `<Application Directory>`. If you do not know where `<Application Directory>` is, see Environment Locations in the Essbase Platform for details.
Linux Example

```
/u01/essbase_data
```

Windows Example

```
z:\essbase_mount
```

> **Note:**
>
> In an environment set up for failover, the application directory must be a shared network mount accessible by both hosts.

c. At the prompt, enter the primary node's domain name. This must match the values you provided during configuration.

Example

```
/scratch/user/oracle_home/user_projects/domains/essbase_domain
```

Once you have provided all the inputs to the script, it finishes configuring failover for the secondary node.

**Additional Configurations**

1. On both nodes, update the managed server startup properties to reference the Oracle HTTP Server (OHS) load balancer host name and port.
   a. Configure OHS entries for primary and secondary nodes using the steps documented in Configure a Load Balancer to Support Failover.
   b. On both the primary and failover nodes:
      On Linux, edit `<Domain Home>\bin\setStartupEnv.sh`

      On Windows, edit `<Domain Home>\bin\setStartupEnv.cmd`

      - Search for the string `DISCOVERY_URL` for the `ESSBASE-MAN-SVR` startup group, and change the hostname and port to the Oracle HTTP Server URL.
        Example

        ```
        -DDISCOVERY_URL=http(s)://OHS_HOST:OHS_PORT/essbase/agent
        ```

      - If Essbase Administration Services (EAS Lite) is also enabled, edit the file `<Domain Home>/bin/setStartupEnv.sh` (on Linux) or `<Domain Home>\bin\setStartupEnv.cmd` (on Windows):
        i. Search for "DISCOVERY_URL" for ESSBASE-EAS-SVR startup group (not ESSBASE-MAN-SVR).
        ii. Change DISCOVERY_URL to point to the Oracle HTTP Server URL.

        ```
        -DDISCOVERY_URL=http(s)://OHS_HOST:OHS_PORT/essbase/agent
        ```

2. Start and validate Essbase Failover Configuration using the steps in Start and Validate the Essbase Failover Configuration.

## Configure TLS for Essbase Failover

Configuring Essbase failover to work with secure mode involves ensuring the keystore configuration matches on both Essbase domains.

You can use the TLS Configuration Utility to update the security certificates for all Essbase nodes and WebLogic managed servers. Beginning with Release 21.4, this utility is available so that you do not need to manually duplicate the identity and trust store configurations on all clients and servers.

To use the utility, follow the instructions in **TLS Configuration Utility**; otherwise, to configure manually, see **Manual TLS Configuration**.

**TLS Configuration Utility**

The following steps are applicable only if you are using the default self-signed certificates. For failover to work, you must update the TLS certificates for all Essbase nodes and WebLogic managed servers.

The command-line steps are for example purposes only. Details of your environment will vary.

**Prerequisites**

- Essbase was configured for Secure Connection Mode during the WebLogic Server Ports Configuration phase of the deployment.
- Essbase servers are stopped (see Stop, Start, and Check Servers).

1. On the machine where the primary Essbase node and Fusion Middleware are installed, navigate to `<ORACLE_HOME>/essbase/bin`.

   ```
   cd /scratch/username/oracle_home/essbase/bin
   ```

2. Open `tls_tools.properties` in a text editor. The contents, by default, are the following parameters with empty values:

   ```
   certFile=
   certCA=
   SAN=
   ```

3. Provide values to the SAN parameter to indicate how Essbase should update the certificates. Leave the other parameters blank. If you leave the `tls_tools.properties` file unconfigured, then when you run `tlsTools.jar`, the utility updates all existing certificates in the Essbase environment. However, if you need to enable Essbase for failover, you need more than the default configuration, because you need to include all the nodes needed for the failover environment.

   The SAN (Subject Alternative Name) parameter lets you specify all the IP addresses and domain names that need to be secured by the certificate update. If you are configuring Essbase for failover, provide information to this parameter about all of the following server locations:

   - Each Essbase host in the failover environment
   - The load balancer (for example, if Oracle HTTP Server is used for the load balancer, include that IP address)
   - The EPM Shared Services server, if you are using EPM security mode

   Example:

   ```
   SAN=IP:10.x.x.11,IP:10.x.x.13,IP:10.x.x.17,DNS:myhost,DNS:myhost.example.com
   certCA=
   certFile=
   ```

4. Save the `tls_tools.properties` file.
5. Navigate to the location of the TLS Configuration Utility, `<ORACLE_HOME>/essbase/lib`.

   ```
   cd /scratch/username/oracle_home/essbase/lib
   ```

6. Set the following variables in your current terminal session or shell script (where you will invoke `tlsTools.jar`):

   - JAVA_HOME and PATH
   - ORACLE_HOME
   - DOMAIN_HOME

Linux Example:

```
export JAVA_HOME=/scratch/jdk1.8.0_311
export PATH=$JAVA_HOME/bin:$PATH
export ORACLE_HOME=/scratch/username/oracle_home
export DOMAIN_HOME=/scratch/username/oracle_home/user_projects/domains/
essbase_domain
```

Windows Example:

```
set JAVA_HOME=C:\Program Files(x86)\Java\jdk1.8\
set PATH=%JAVA_HOME%\bin;%PATH%
set ORACLE_HOME=C:\oracle_home
set DOMAIN_HOME=C:\oracle_home\user_projects\domains\essbase_domain
```

7. Run the TLS Configuration Utility, providing as an argument the path to the TLS properties file.

   On Linux:

   ```
   java -jar $ORACLE_HOME/essbase/lib/tlsTools.jar $ORACLE_HOME/essbase/bin/
   tls_tools.properties
   ```

   On Windows:

   ```
   java -jar %ORACLE_HOME%\essbase\lib\tlsTools.jar %ORACLE_HOME%
   \essbase\bin\tls_tools.properties
   ```

   The utility prompts you for your private key password.

   The utility replaces the certificates in the identity and trust stores, depending on how you configured the properties file.

### Manual TLS Configuration

The following steps are applicable only if you are using the default self-signed certificates. If you updated certificates using the TLS Configuration Utility (`tlsTools.jar`), then you can skip these steps.

For Host 1 and Host 2 SSL/TLS configuration, see About Securing Your Communication and Network.

1. If WebLogic managed server is configured for SSL/TLS, then you need to copy the following files from Host 1 to the same directories on Host 2:

   ```
   DOMAIN_HOME/config/fmwconfig/essconfig/essbase/walletssl/keystore.jks
   ```

   ```
   DOMAIN_HOME/config/fmwconfig/ovd/default/keystores/adapters.jks
   ```

2. Start the WebLogic AdminServer on Host 1.

   On Linux:

   ```
   DOMAIN_HOME/esstools/bin/start.sh -i AdminServer
   ```

On Windows:

```
DOMAIN_HOME\esstools\bin\start.cmd -i AdminServer
```

3. Log in to the WebLogic administration console on Host 1. In the Domain Structure tree on the left, navigate to **domain name** -> **Environment** ->**Servers** -> **essbase_server1** ->**Configuration** tab ->**Keystores** tab.
4. Record the configuration values for **Custom Identity Keystore** and **Custom Trust Keystore**.
5. From the **Configuration**->**SSL** tab, record the value of the **Private Key** alias for **essbase_server1**.
6. Lock and edit the configuration.
7. Set the same values for **essbase_server2** in corresponding **Keystores** and **SSL** tabs, after changing keystores to 'Custom Identity and Custom Trust.'
   a. Navigate to **Environment** ->**Servers** -> **essbase_server2** ->**Configuration** tab ->**Keystores** tab.
   b. Click the **Change** button next to **Demo Identity and Demo Trust**.
   c. In the **Keystores** drop-down menu, select **Custom Identity and Custom Trust**, and click **Save**.
   d. For **Custom Identity Keystore**, paste the configuration path to `keystore.jks` that you recorded from essbase_server1 configuration.
   e. For **Custom Trust Keystore**, paste the configuration path to `adapters.jks` that you recorded from essbase_server1 configuration.
   f. Click **Save**.
   g. Click the **SSL** tab.
   h. For **Private Key Alias**, paste the alias that you recorded, and click **Save**.
8. Save and activate the changes.
9. Make sure both of the managed server certificates are imported into the trust store of the load balancer.

## Oracle HTTP Server Configuration for Essbase

Failover configurations require a front-end load balancer.

One option to consider for a load balancer is Oracle HTTP Server, because it is integrated with WebLogic and provides web services for Fusion Middleware.

See Configure a Load Balancer to Support Failover.

## Start and Validate the Essbase Failover Configuration

Confirm that the failover configuration works by starting and then validating it.

**Start the Failover Configuration**

1. Start the Node Manager on node 2.
   a. Check whether Node Manager is running.
      - On Linux, SSH to Node 2 and check whether Node Manager is running using `ps -lf | grep NodeManager`.

- On Windows, check the java process in Task Manager.

b. If it is not running, start it
On Linux:

```
<Domain Home>/bin/startNodeManager.sh &
```

On Windows:

```
<Domain Home>\bin\startNodeManager.cmd &
```

2. SSH to Host 1 and restart Essbase (the AdminServer and both the managed servers) as described in Stop, Start, and Check Servers.

> **Note:**
>
> In EPM deployments only, the EPM WebLogic Server should be started before starting the Essbase managed server.

In order to start and stop each server individually, use the -i parameter with server name.

Linux Example:

```
<Domain Home>/esstools/bin/start.sh -i essbase_server1
```

```
<Domain Home>/esstools/bin/stop.sh -i essbase_server1
```

Windows Example:

```
<Domain Home>\esstools\bin\start.cmd -i essbase_server1
```

```
<Domain Home>\esstools\bin\stop.cmd -i essbase_server1
```

To check the node status, use,

On Linux:

```
<Domain Home>/esstools/bin/status.sh
```

On Windows:

```
<Domain Home>\esstools\bin\status.cmd
```

3. Log in to the admin console of Host 1.
4. Click on the **<Domain Name>** -> **Environment** -> **Servers** link and verify that both the Essbase managed servers are shown as RUNNING.

**Validate the Failover Configuration**

1. Log in to the Essbase admin console using the Oracle HTTP Server link: `http(s)://`*`OHS_Host_Name`*`:`*`OHS_Port`*`/essbase/jet`.

2. Manually stop the active node using,
On Linux:

```
stop.sh -i managed_server_name
```

On Windows:

```
stop.cmd -i managed_server_name
```

To validate that the failover node takes over, manually stop the active node using `stop.sh` (Linux) or `stop.cmd` (Windows).

Linux Example:

```
stop.sh -i essbase_server1
```

Windows Example:

```
stop.cmd -i essbase_server1
```

The Essbase clients require a new login after every node switch.

> **Note:**
>
> Essbase is not accessible for a few seconds during the transition from the active node to the passive node. The length of time depends on the configuration settings, AGENTLEASEEXPIRATIONTIME and AGENTLEASERENEWALTIME.

## Essbase Failover Post Configuration Tasks

After configuration, you may want to patch the nodes, or make custom changes to configuration files.

**Patching Nodes**
To patch the nodes with the latest binaries, follow the steps in Patch and Roll Back, applying opatches to each node.

> **Note:**
>
> Perform the start and stop operations mentioned in the above link only from the primary node.

**Additional Steps if Making Custom essbase.cfg, esssql.cfg or odbc.ini Changes**
Make any changes needed in essbase.cfg, esssql.cfg, or odbc.ini under `<Domain Home>`. Do this only on the primary node, Host 1, and restart the managed servers to avoid any inconsistency between applications. Use one of the following methods:

- Shut down the cluster completely, make changes to the essbase.cfg, esssql.cfg, or odbc.ini file on the primary node, and then restart everything. This avoids any inconsistency between applications, but it results in more down time.

- Shutdown servers on primary node, make changes to the essbase.cfg, esssql.cfg or odbc.ini file, and restart servers. Once node 1 is restarted, restart node 2. This results in less down time.

## Manual Steps for Essbase Failover Configuration on the Primary Node (Host 1)

**Tip**: For Release 21.5.2 or higher, skip these instructions and use the instructions in Set up an Essbase Failover Environment Using the Failover Setup Script instead.

Configure the primary Essbase node for failover. You will run the Fusion Middleware configuration wizard, edit script files, add Essbase configuration properties, configure servers in the WebLogic Console, run the TLS tools utility, pack the domain configuration, and copy it to the second node.

Before you begin, review Configure TLS for Essbase Failover to learn how to configure the TLS properties file.

Host 1 is the primary Essbase node and has all services not clustered (such as AdminServer and, optionally, EAS Lite).

1. SSH to Host 1 and stop the Essbase instance:

   On Linux:

   ```
   <Domain Home>/esstools/bin/stop.sh
   ```

   On Windows:

   ```
   <Domain Home>\esstools\bin\stop.cmd
   ```

2. Launch the Fusion Middleware (FMW) configuration wizard and update the configuration on Host 1:

   On Linux:

   ```
   <Oracle Home>/oracle_common/common/bin/config.sh
   ```

   On Windows:

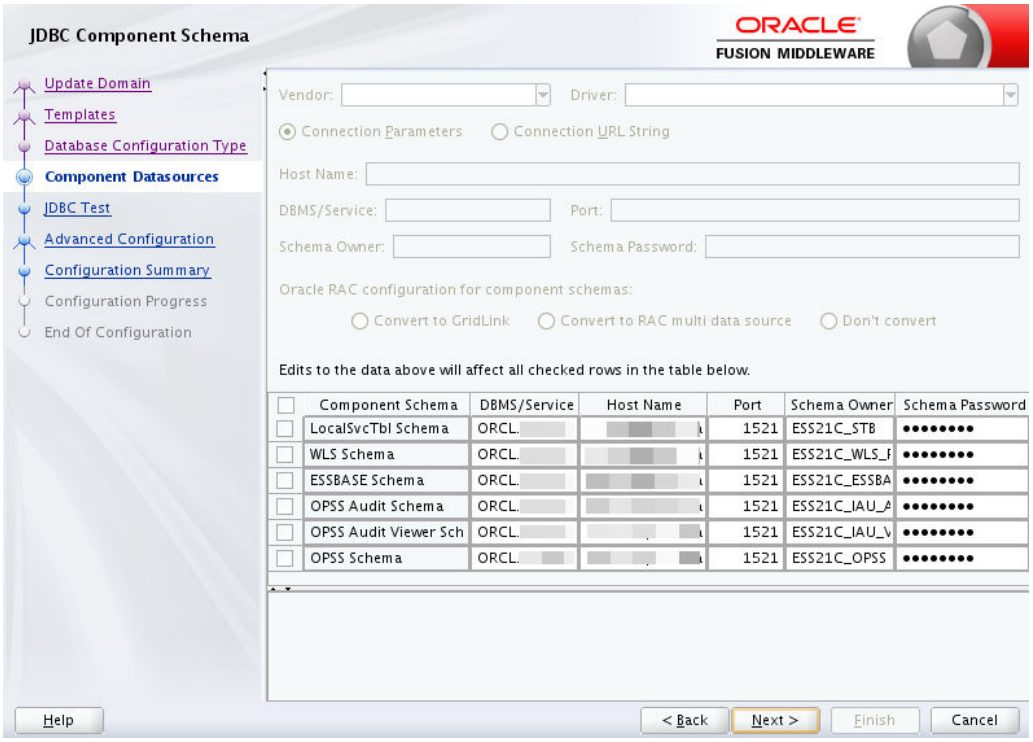
   ```
   <Oracle Home>\oracle_common\common\bin\config.cmd
   ```

   a. On the **Create Domain** screen, select **Update an existing domain**. Make sure the correct domain location is specified in the **Domain Location** field, and click **Next**.

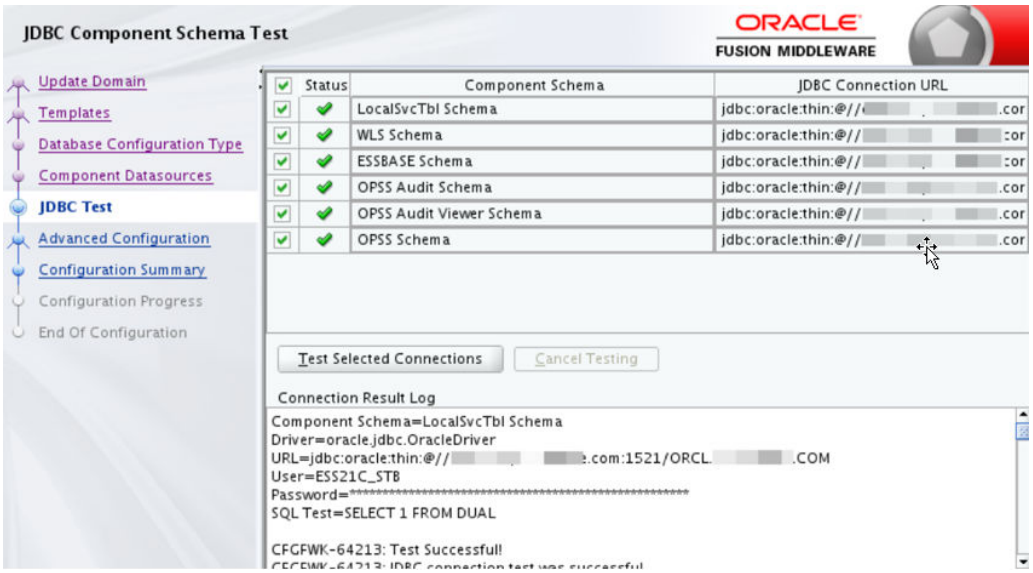
   b. On the **Templates** screen, accept the defaults and click **Next**.

   c. On the **Database Configuration Type** screen, change the selection from **RCU Data** to **Manual Configuration** and click **Next**.

   d. On the **Component Datasources** screen, accept the defaults and click **Next**.

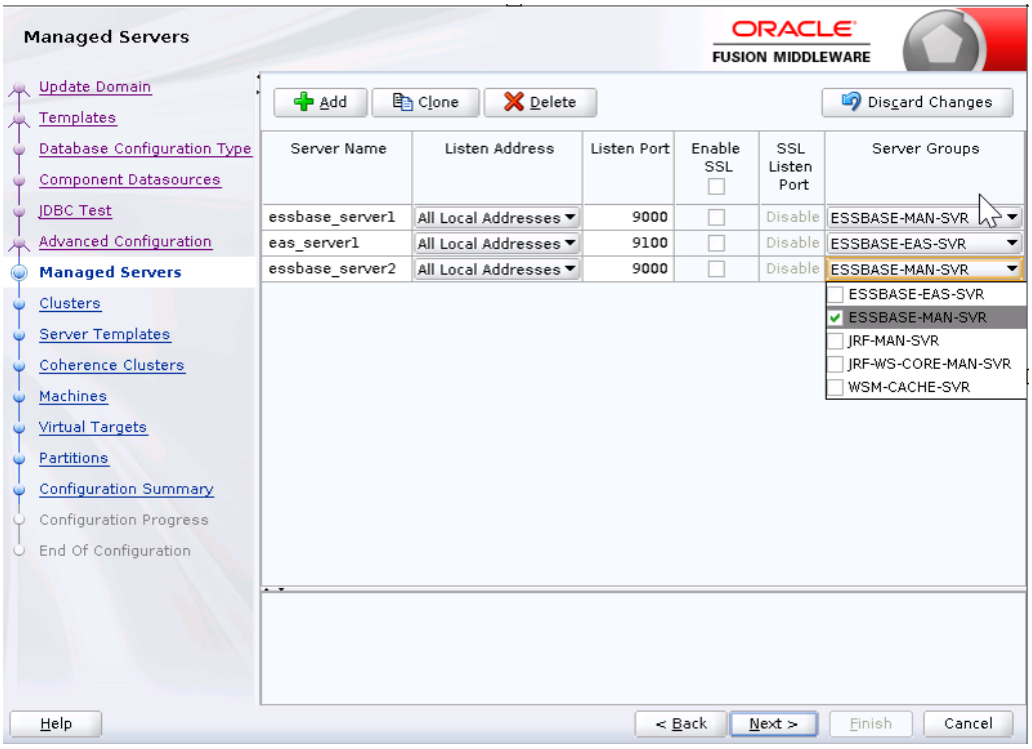



e. On the **JDBC Test** screen, accept the defaults and click **Next**.




f. On the **Advanced Configuration** screen, select **Topology** and click **Next**.

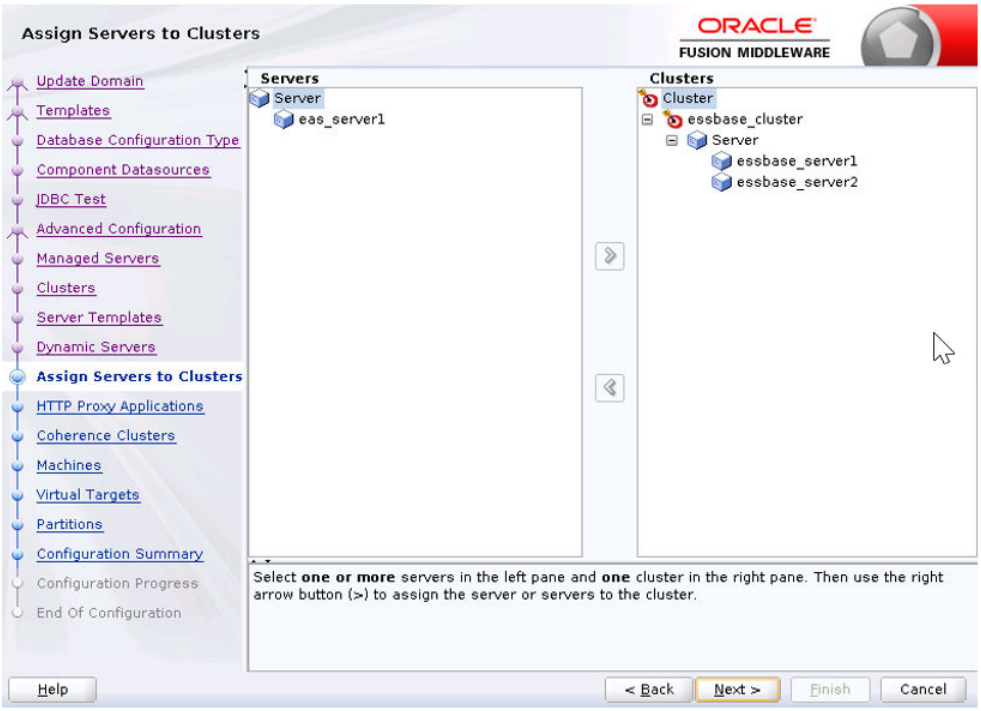
g. On the **Managed Servers** screen, click **Add** and enter the details of Host 2.




- Enter the managed server ports for **essbase_server2**.
- Select the **Enable SSL** check box if you need to update the SSL Listen Port.
- To update the SSL Listen Port, click the **Listen Port** input box. Select the server groups as **ESSBASE-MAN-SVR** and click **Next**.

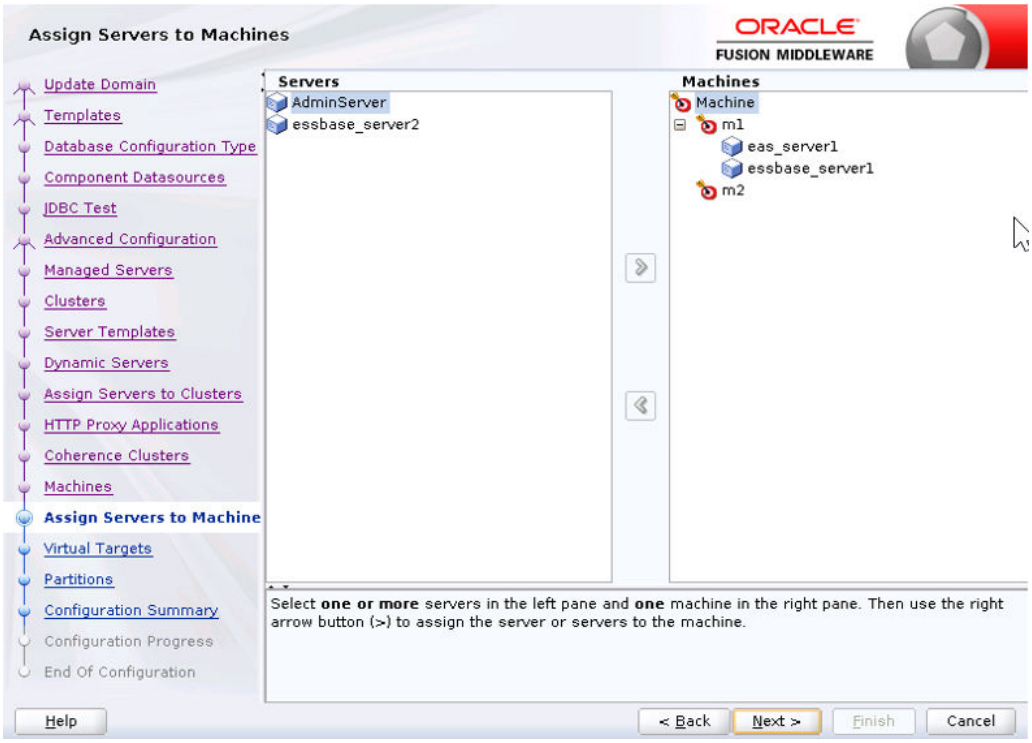
**h.** Accept the defaults and click **Next** on the following screens:

- **Clusters**
- **Server Templates**
- **Dynamic Servers**
- **Assign Servers to Clusters**

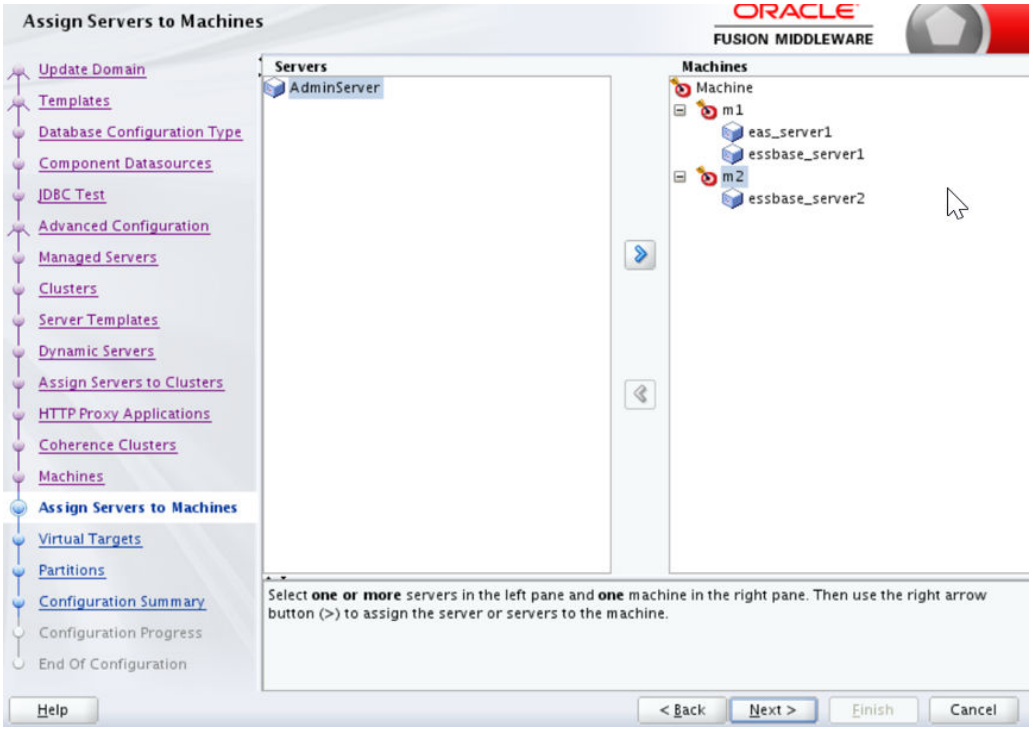



- **HTTP Proxy Applications**
- **Coherence Clusters**

i. On the **Machines** screen, click **Add** and add a new machine, **m2**. Enter the Host 2 hostname and Node Manager port values. You can choose the Node Manager port, 9556. Click **Next**.



j. On the **Assign Servers to Machines** screen, select **m2** in the right hand panel. Select the newly created server, **essbase_server2** in the left hand panel and add it to **m2**. After adding it, **essbase_server2** is displayed under **m2**. Click **Next**.




k. Accept the defaults and click next on the following screens:
   - **Virtual Targets**
   - **Partitions**

l. On the **Configuration Summary** screen, click **Update**.

m. When the update is done, click **Next**, and in the last screen, click **Finish** to complete the configuration changes.

3. On Host 1, edit the file `<Domain Home>/bin/setDomainEnv.sh` (on Linux) or `<Domain Home>\bin\setDomainEnv.cmd` (on Windows).

> **Caution:**
>
> The Essbase platform includes scripts in `<DOMAIN HOME>/bin` that can customize the environment and behaviors of Essbase functionality. However, making changes to these domain environment or startup scripts can have unintended effects, including startup failure. Oracle recommends making changes in a test environment first. Before editing these scripts, always:
>
> a. Stop the Essbase managed servers, using `<DOMAIN HOME>/esstools/bin/stop.sh` (on Linux), or `<DOMAIN HOME>\esstools\bin\stop.cmd`(on Windows).
>
> b. In `<DOMAIN HOME>/bin`, make a backup copy of the file you want to edit. For example,
>
> On Linux
>
> ```
> cp setStartupEnv.sh setStartupEnv_bak.sh
> ```
>
> On Windows
>
> ```
> copy setStartupEnv.cmd setStartupEnv_bak.cmd
> ```
>
> c. Edit carefully, using only Oracle's documented instructions, or working with Oracle Support.
>
> d. Restart Essbase, using `<DOMAIN HOME>/esstools/bin/start.sh` (on Linux), or `<DOMAIN HOME>\esstools\bin\start.cmd`(on Windows). Check that startup completed normally.

a. Search for the string `EXTRA_JAVA_PROPERTIES`.

**Important**: Search for `EXTRA_JAVA_PROPERTIES`, not `JAVA_PROPERTIES`.

b. Add the following -D definition after the existing export `EXTRA_JAVA_PROPERTIES` line:

On Linux:

```
EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES}-
Dweblogic.security.SSL.ignoreHostnameVerification=true" export
EXTRA_JAVA_PROPERTIES
```

On Windows:

```
set EXTRA_JAVA_PROPERTIES=-
Dweblogic.security.SSL.ignoreHostnameVerification=true
%EXTRA_JAVA_PROPERTIES%
```

> **Note:**
>
> This step is not required if all the TLS certificates are imported properly. In case of self-signed certificates, or if the managed server later fails to start with SSL errors, this step is required.

4. Edit the file, `<Domain Home>/config/fmwconfig/essconfig/essbase/essbase.cfg`, and add the following lines:

   FAILOVERMODE true

   #Optional

   AGENTLEASERENEWALTIME 10

   #Optional

   AGENTLEASEEXPIRATIONTIME 20

5. If Essbase Administration Services (EAS Lite) is also enabled, edit the file `<Domain Home>/bin/setStartupEnv.sh` (on Linux) or `<Domain Home>\bin\setStartupEnv.cmd` (on Windows):

   a. Search for "DISCOVERY_URL" for ESSBASE-EAS-SVR startup group (not ESSBASE-MAN-SVR).

   b. Change DISCOVERY_URL to point to the Oracle HTTP Server URL.

   ```
   -DDISCOVERY_URL=http(s)://OHS_HOST:OHS_PORT/essbase/agent
   ```

6. Start AdminServer in Host 1.

   On Linux:

   ```
   <Domain Home>/esstools/bin/start.sh -i AdminServer
   ```

   On Windows:

   ```
   <Domain Home>\esstools\bin\start.cmd -i AdminServer
   ```

7. Find out the public IP of both the Host 1 and Host 2 machines, for example, by using the ping command from the other host. If both the machines are behind the firewall, make sure you know the IPs with which both Host 1 and Host 2 can communicate with each other.

8. Configure the AdminServer and the managed servers using WebLogic Console:

   a. Log in to the WebLogic AdminServer console using WebLogic admin credentials. The default AdminServer port is 7001.

      Example: `http(s)://host:7001/console`

   b. Click **Lock & Edit** in the left panel. Navigate to **<Domain Name>** -> **Environment** -> **Servers** -> **AdminServer**. On the **Configuration** tab, click **General** and expand the **Advanced** section. Enter the public IP address of Host 1 in the **External Listen Address** property.

      **Important**: Enter Host 1's IP as seen by Host 2.

   c. Click **Save**.

   d. Repeat steps a, b, and c directly above to update the **External Listen Address** for **essbase_server1** with the Public IP of Host 1.

   e. Remove essbase_cluster from default coherence cluster membership.

      i. Navigate to **<Domain Name>** -> **Environment** -> **Coherence Clusters**.

      ii. Click **defaultCoherenceCluster**. Click the **Members** tab. Deselect **essbase_cluster**.

      iii. Click **Save**.

f. Navigate to **<Domain Name>** -> **Security** tab->**Embedded Ldap** tab. Select the **Master First Option** and click **Save**.

g. Navigate to **<Domain Name>** -> **Environment** -> **Servers**. Click on the newly added server **essbase_server2**.

h. On the **Configuration** tab, navigate to the **General** tab, expand the **Advanced** section then enter the public IP address of Host 2 in the **External Listen Address** field. Make sure you obtain this Public IP by pinging Host 2 from Host 1. Click **Save**.

i. On the **Configuration** tab, navigate to the **General** tab, remove the value from **Listen Address** field and click **Save**.

j. Navigate to **<Domain Name>** -> **Environment** -> **Servers**. Click **essbase_server1**. On the **Configuration** tab, navigate to the **General** tab and remove the value from **Listen Address** field. Click **Save**.

k. In the panel on the left, click **Activate Changes**.

l. Shut down WebLogic in Host 1 using `stop.sh` (on Linux) or `stop.cmd` (on Windows).

   On Linux:

   ```
   <Domain Home>/esstools/bin/stop.sh
   ```

   On Windows:

   ```
   <Domain Home>\esstools\bin\stop.cmd
   ```

9. Run `tlsTools.jar` to update certificates, as described in Configure TLS for Essbase Failover.

10. In Host 1, pack the complete domain configuration by running the following command, and export it as a jar file. This could take few minutes.

    On Linux:

    ```
    <Oracle home>/oracle_common/common/bin/pack.sh -domain=<DOMAIN_HOME> -
    template=<user specified path>/essbase_ha.jar -
    template_name=essbase_domain -managed=true
    ```

    Linux Example:

    ```
    ./Oracle/Middleware/Oracle_Home/oracle_common/common/bin/pack.sh -domain=./
    Oracle/Middleware/Oracle_Home/user_projects/domains/essbase_domain -
    template=./essbase_ha.jar -template_name=essbase_domain -managed=true
    ```

    On Windows:

    ```
    <Oracle home>\oracle_common\common\bin\pack.cmd -domain=<DOMAIN_HOME> -
    template=<user specified path>/essbase_ha.jar -
    template_name=essbase_domain -managed=true
    ```

Windows Example:

```
c:\>\Oracle_Home\oracle_common\common\bin\pack.cmd -
domain=C:\Oracle_Home\user_projects\domains\essbase_domain -
template=essbase_ha.jar -template_name=essbase_domain -managed=true
```

11. Transfer the generated jar, `<user specified path>/essbase_ha.jar` to a folder in the secondary node.
    - On Linux, use network copy or ftp:

      ```
      cp /network path of Host 1/<Host 1 Essbase Installation>/essbase_ha.jar
      <Host 2>/<some dir>/essbase_ha.jar
      ```

    - On Windows, copy the `essbase_ha.jar` to the second node by sharing the folder between the two nodes.

## Manual Steps for Failover Configuration on the Secondary Node (Host 2)

**Tip**: For Release 21.5.2 or higher, skip these instructions and use the instructions in Set up an Essbase Failover Environment Using the Failover Setup Script instead.

Host 2, the secondary node, only runs Essbase.

1. SSH to the secondary node, Host 2.
2. Run WebLogic and unpack `essbase_ha.jar`, which you copied from Host 1.
   On Linux:

   ```
   <Oracle home>/oracle_common/common/bin/unpack.sh -template=essbase_ha.jar -
   domain=<Domain Home>
   ```

   Linux Example:

   ```
   ./Oracle/Middleware/Oracle_Home/oracle_common/common/bin/unpack.sh -
   template=/scratch/essbase_ha.jar -domain=<Domain Home>
   ```

   On Windows:

   ```
   <Oracle home>\oracle_common\common\bin\unpack.cmd -template=essbase_ha.jar
   -domain=<Domain Home>
   ```

   Windows Example:

   ```
   .\Oracle\Middleware\Oracle_Home\oracle_common\common\bin\unpack.cmd -
   template=\scratch\essbase_ha.jar -domain=<Domain Home>
   ```

> **Note:**
>
> `<Domain Home>` should be exactly the same as defined in Host 1. For example, `./Oracle/Middleware/Oracle_Home/user_projects/domains/essbase_domain`

3. Edit `<Domain Home>/bin/setDomainEnv.sh` (on Linux) or `<Domain Home>\bin\setDomainEnv.cmd` (on Windows)

> **Caution:**
>
> The Essbase platform includes scripts in `<DOMAIN HOME>/bin` that can customize the environment and behaviors of Essbase functionality. However, making changes to these domain environment or startup scripts can have unintended effects, including startup failure. Oracle recommends making changes in a test environment first. Before editing these scripts, always:
>
> a. Stop the Essbase managed servers, using `<DOMAIN HOME>/esstools/bin/stop.sh` (on Linux), or `<DOMAIN HOME>\esstools\bin\stop.cmd`(on Windows).
>
> b. In `<DOMAIN HOME>/bin`, make a backup copy of the file you want to edit. For example,
>
> On Linux
>
> ```
> cp setStartupEnv.sh setStartupEnv_bak.sh
> ```
>
> On Windows
>
> ```
> copy setStartupEnv.cmd setStartupEnv_bak.cmd
> ```
>
> c. Edit carefully, using only Oracle's documented instructions, or working with Oracle Support.
>
> d. Restart Essbase, using `<DOMAIN HOME>/esstools/bin/start.sh` (on Linux), or `<DOMAIN HOME>\esstools\bin\start.cmd`(on Windows). Check that startup completed normally.

Similarly to how EXTRA_JAVA_PROPERTIES was added to Host 1, copy the same EXTRA_JAVA_PROPERTIES to `setDomainEnv.sh` (on Linux), or `setDomainEnv.cmd` (on Windows) in Host 2.

a. Search for the string `EXTRA_JAVA_PROPERTIES`.

   **Important**: Search for `EXTRA_JAVA_PROPERTIES`, not `JAVA_PROPERTIES`.

b. Add the following -D definition after the existing export `EXTRA_JAVA_PROPERTIES` line:

   On Linux:

   ```
   EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES}-
   Dweblogic.security.SSL.ignoreHostnameVerification=true" export
   EXTRA_JAVA_PROPERTIES
   ```

   On Windows:

   ```
   set EXTRA_JAVA_PROPERTIES=-
   Dweblogic.security.SSL.ignoreHostnameVerification=true
   %EXTRA_JAVA_PROPERTIES%
   ```

> **Note:**
>
> This step is not required if all the TLS certificates are imported properly. In case of self-signed certificates, or if the managed server later fails to start with SSL errors, this step is required.

4. Edit `<Domain Home>/bin/setStartupEnv.sh` (on Linux) or `<Domain Home>\bin\setStartupEnv.cmd` (on Windows).
   Search for "DISCOVERY_URL" for ESSBASE-MAN-SVR startup group and change the hostname and port from the Host 1 values to the Host 2 values.

   > **Note:**
   >
   > Modify this only for ESSBASE-MAN-SVR. If Essbase Administration Services is installed, then DISCOVERY_URL for ESSBASE-EAS-SVR as STARTUP-GROUP should be `https://OHS_HOST:OHS_PORT/essbase/agent`.
   > `-DDISCOVERY_URL=https://Host 2:port/essbase/agent`

5. Check the listen address in `nodemanager.properties` by editing `<Domain Location/<Domain Name>/nodemanager/nodemanager.properties`. Make sure `ListAddress` points to Host 2.

## Set Up Admin Server Failover

Essbase in independent deployment runs as a managed server, and depends on the WebLogic Administration Server in order to start, stop, and go into failover mode in case of failure on the primary node.

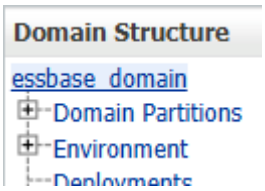
You can set up Essbase in failover mode on more than one host, in case the primary host becomes unavailable. In addition, it is recommended that you set up the WebLogic Administration Servers for high availability, to ensure that Essbase failover nodes can initialize.

This topic contains guidelines to set up AdminServer high availability with an Essbase failover configuration. For general information about WebLogic AdminServer high availability, refer to Administration Server High Availability.

### Preconfigure High Availability of Essbase Managed Servers

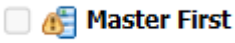
To enable high availability for WebLogic managed servers used for Essbase, complete the following configuration.

1. Log in to the WebLogic Server Admininstration Console.
2. On the home page, under Domain Structure, click the Essbase domain name (for example, essbase_domain).



3. Navigate, using the tabs, to Security > Embedded LDAP.


4. Unselect the following option, and click Save.




5. SSH to Host 1 and restart Essbase (the AdminServer and both the managed servers) as described in Stop, Start, and Check Servers.

> **Note:**
>
> In EPM Shared Services deployments only, the EPM WebLogic Server should be started before starting the Essbase managed server.

In order to start and stop each server individually, use the -i parameter with server name.

Linux Example (start):

```
<Domain Home>/esstools/bin/start.sh -i essbase_server1
```

Windows Example (start):

```
<Domain Home>\esstools\bin\start.cmd -i essbase_server1
```

### Set Up Admin Server High Availability

#### Prerequisites

- You have completed the Essbase Failover Prerequisites.
- You have a shared network drive that is accessible to both (or all) Essbase hosts that you configured for failover. It can be the same location mentioned in Essbase Failover Prerequisites.

To set up WebLogic Admin Server high availability with an Essbase failover environment,

1. Create a virtual IP address (VIP) on the primary node (Host 1).

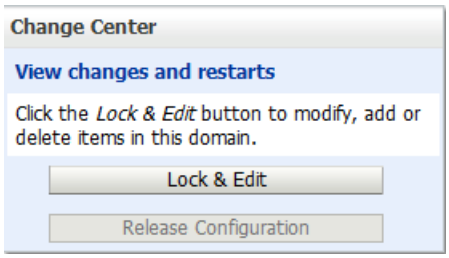
   Use the Linux **ip** command. The syntax is:

   ```
   ip addr add <VIP>/<NETMASK> dev <INTERFACE> label <LABEL_NAME>
   ```

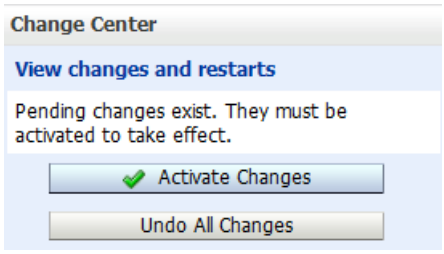
Example:

```
ip addr add 100.xx.xx.1/20 dev ens3 label ens3:2
```

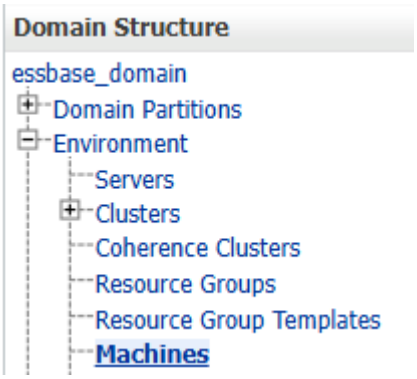
2. Set up the Essbase failover environment, as described in Set up an Essbase Failover Environment Using the Failover Setup Script.
3. Test that the Essbase failover environment setup was successful (refer to Start and Validate the Essbase Failover Configuration).
4. Log in to the WebLogic Server Admininstration Console.
5. On the Home page, under Domain Configurations > Environment, navigate to Servers, and click AdminServer.
6. In the Change Center pane, click **Lock & Edit**.



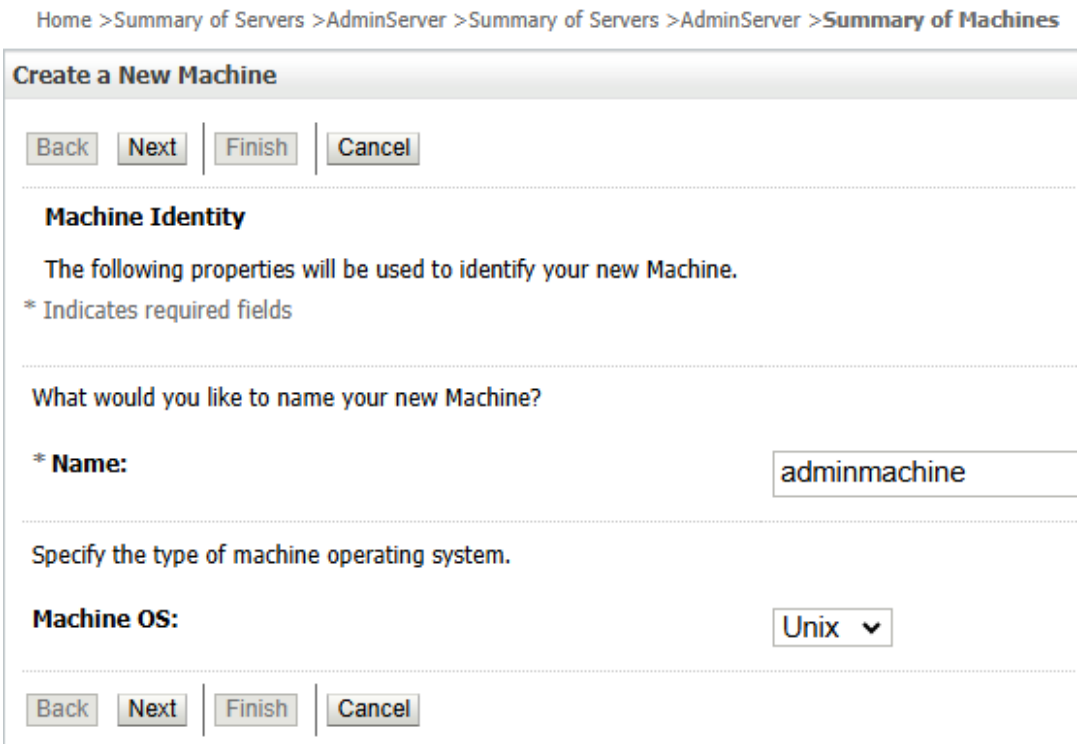

7. Change the Listen Address to the virtual IP (VIP) address.
8. Click **Save**.
9. Click **Activate Changes**.



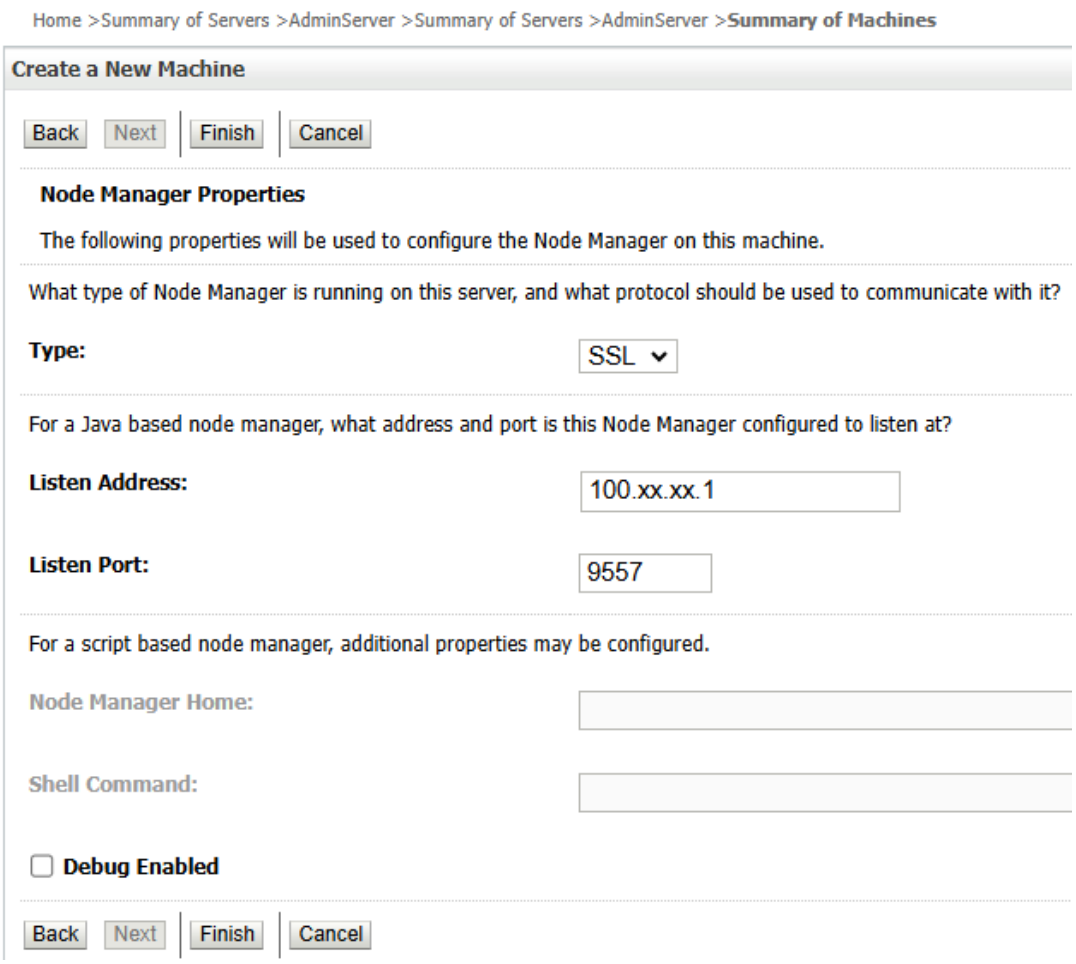

10. Restart the Admin Server.
11. Log in again to the WebLogic Server Admininstration Console.
12. Under the domain structure, navigate to Environment > Machines.



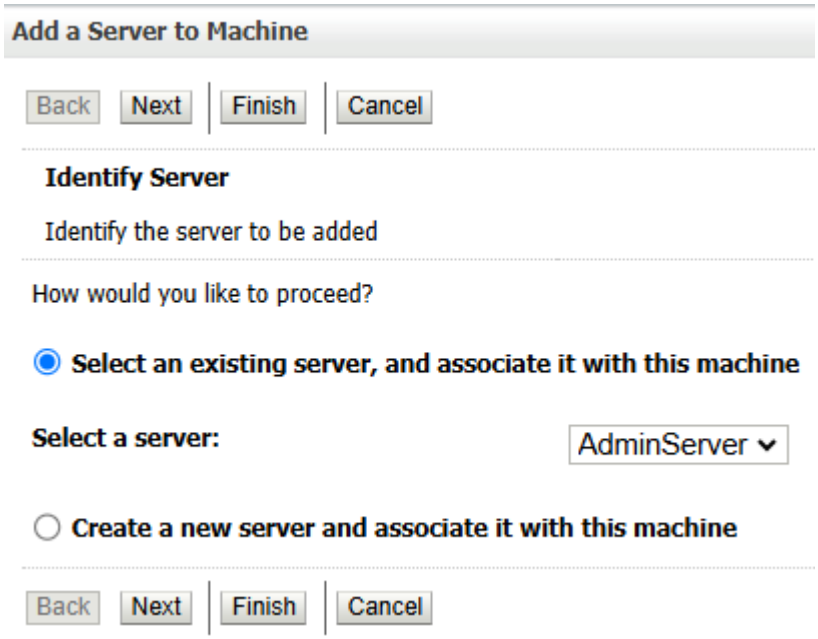

13. Click **Lock & Edit**, then click New to add a new machine named adminmachine. Set the Machine OS as Unix, and click Next.




14. Set the Node Manager type to SSL, set the Listen Address to the virtual IP (VIP) address, and set the port to 9557. Click Finish.




15. In the **Summary of Machines** table, click the link for the new **adminmachine**, and click the **Configuration** tab, then the **Servers** tab.
16. Click Add, select **AdminServer**, and click Finish.




17. SSH to the Essbase primary node (Host 1), navigate to `<Domain_Home>/servers/AdminServer`, and make a directory `nodemanager`.
18. Navigate into `nodemanager` directory and create two new files, `nodemanager.domains` and `nodemanager.properties`.

    Sample of `nodemanager.domains` (replace the value to match your own installed Essbase domain name and path):

    ```
    essbase_domain=/u01/oracle/user_projects/domains/essbase_domain
    ```

    Sample of `nodemanager.properties` (replace the value to match your own installed Essbase domain name and path):

    ```
    DomainsFile=/u01/oracle/user_projects/domains/essbase_domain/servers/
    AdminServer/nodemanager/nodemanager.domains
    LogLimit=0
    PropertiesVersion=12.2.1.1.0
    AuthenticationEnabled=true
    NodeManagerHome=/u01/oracle/user_projects/domains/essbase_domain/servers/
    AdminServer/nodemanager
    JavaHome=/u01/app/oracle/product/JAVA/jdk
    LogLevel=INFO
    DomainsFileEnabled=true
    ListenAddress=100.xx.xx.1
    NativeVersionEnabled=true
    ListenPort=9557
    LogToStderr=true
    weblogic.StartScriptName=startWebLogic.sh
    SecureListener=true
    LogCount=1
    QuitEnabled=false
    LogAppend=true
    weblogic.StopScriptEnabled=false
    ```

```
StateCheckInterval=500
CrashRecoveryEnabled=false
weblogic.StartScriptEnabled=true
LogFile=/u01/oracle/user_projects/domains/essbase_domain/servers/
AdminServer/nodemanager/nodemanager.log
LogFormatter=weblogic.nodemanager.server.LogFormatter
ListenBacklog=50
```

19. Navigate to `<Domain_Home>/bin`. Example:

    ```
    cd /u01/oracle/user_projects/domains/essbase_domain/bin
    ```

20. Make a copy of the Node Manager startup script, with a new name `startNodeManagerAdmin.sh`. Example:

    ```
    cp startNodeManager.sh startNodeManagerAdmin.sh
    ```

21. Open `startNodeManagerAdmin.sh` for editing. Change the value of NODEMGR_HOME to "`<Domain_Home>/servers/AdminServer/nodemanager`", and save the file. Example:

    ```
    NODEMGR_HOME="/u01/oracle/user_projects/domains/essbase_domain/nodemanager"
    ```

22. Navigate to `<Domain_Home>/esstools/bin`. Example:

    ```
    cd /u01/oracle/user_projects/domains/essbase_domain/esstools/bin
    ```

23. Stop the AdminServer. Example:

    ```
    ./stop.sh -i AdminServer
    ```

24. Navigate back to `<Domain_Home>/bin` and run `startNodeManagerAdmin.sh` in the background. Example:

    ```
    cd /u01/oracle/user_projects/domains/essbase_domain/bin
    ./startNodeManagerAdmin.sh &
    ```

25. Set the domain environment. Example:

    ```
    source /u01/oracle/user_projects/domains/essbase_domain/bin/setDomainEnv.sh
    ```

26. Run the WebLogic Scripting Tool, located in `<ORACLE_HOME>/oracle_common/common/bin`. Example:

    ```
    /u01/oracle/user_projects/oracle_common/common/bin/wlst.sh
    ```

27. At the `wls:/offline>` prompt, connect to Node Manager, then start the AdminServer. For example, use the following commands (replace <*variables*> with your values):

    ```
    wls:/offline>
    nmConnect('<WebLogic_admin_user>','<WebLogic_admin_password>', '<Virtual-
    IP-address>','9557','<DOMAIN_NAME>','<DOMAIN_HOME>','ssl')
    wls:/nm/mydomain> nmStart('AdminServer')
    ```

Example:

```
wls:/offline> nmConnect('wladmin','wlpa55w0rD',
'<100.xx.xx.1>','9557','essbase_domain','/u01/oracle/user_projects/domains/
essbase_domain','ssl')
wls:/nm/mydomain> nmStart('AdminServer')
```

28. Keeping wlst open, check that you can access the WebLogic Server Administrative console using the virtual IP address. For example, `http://100.xx.xx.1:7001/console`.
29. Stop the AdminServer.

```
wls:/nm/mydomain> nmKill('AdminServer')
```

30. Exit the WebLogic Scripting Tool. Example:

```
exit()
```

31. Go to the shared network drive and make a new directory with the same name as your Essbase <*DOMAIN_NAME*>. Example:

```
cd /nfs/essbase_data
mkdir essbase_domain
```

32. Move Essbase domain subdirectories `bin`, `config`, and `/servers/AdminServer` to the new directory on the shared drive. Example:

```
mv /u01/oracle/user_projects/domains/essbase_domain/bin /nfs/essbase_data/
essbase_domain/
mv /u01/oracle/user_projects/domains/essbase_domain/config /nfs/
essbase_data/essbase_domain/
mv /u01/oracle/user_projects/domains/essbase_domain/servers/
AdminServer /nfs/essbase_data/essbase_domain/
```

33. Navigate back to <*Domain_Home*> and make symbolic links to the Essbase domain folders on the shared drive. Example:

```
cd /u01/oracle/user_projects/domains/essbase_domain/
ln -s /nfs/essbase_data/essbase_domain/bin .
ln -s /nfs/essbase_data/essbase_domain/config .
cd servers/
ln -s /nfs/essbase_data/essbase_domain/AdminServer .
```

34. SSH to the Essbase secondary node (Host 2), navigate to <*Domain_Home*>, and make a directory structure `/tmp/admin`. Example:

```
cd /u01/oracle/user_projects/domains/essbase_domain
mkdir /tmp/admin
```

35. Move domain subdirectories `bin`, `config`, and `/servers/AdminServer` into `/tmp/admin`. Example:

```
mv bin /tmp/admin/
mv config /tmp/admin/
mv ./servers/AdminServer /tmp/admin/
```

36. Make symbolic links to the Essbase domain folders on the shared drive. Example:

```
ln -s /nfs/essbase_data/essbase_domain/bin .
ln -s /nfs/essbase_data/essbase_domain/config .
cd servers/
ln -s /nfs/essbase_data/essbase_domain/AdminServer .
```

### Validate AdminServer High Availability

To validate that you set up WebLogic AdminServer high availability successfully with the Essbase failover environment, test that you can access the WebLogic Server Administrative console, using the virtual IP address, from the Essbase primary node and any failover nodes.

1. SSH to the Essbase primary node (Host 1), navigate to `<Domain_Home>/bin`, and run `startNodeManagerAdmin.sh` in the background. Example:

```
cd /u01/oracle/user_projects/domains/essbase_domain/bin
./startNodeManagerAdmin.sh &
```

2. Set the domain environment. Example:

```
source /u01/oracle/user_projects/domains/essbase_domain/bin/setDomainEnv.sh
```

3. Run the WebLogic Scripting Tool, located in `<ORACLE_HOME>/oracle_common/common/bin`. Example:

```
/u01/oracle/user_projects/oracle_common/common/bin/wlst.sh
```

4. At the `wls:/offline>` prompt, connect to Node Manager, then start the AdminServer. For example, use the following commands (replace <*variables*> with your values):

```
wls:/offline>
nmConnect('<WebLogic_admin_user>','<WebLogic_admin_password>', '<Virtual-IP-address>','9557','<DOMAIN_NAME>','<DOMAIN_HOME>','ssl')
wls:/nm/mydomain> nmStart('AdminServer')
```

   Example:

```
wls:/offline> nmConnect('wladmin','wlpa55w0rD',
'<100.xx.xx.1>','9557','essbase_domain','/u01/oracle/user_projects/domains/essbase_domain','ssl')
wls:/nm/mydomain> nmStart('AdminServer')
```

5. Check that you can access the WebLogic Server Administrative console using the virtual IP address. For example, `http://100.xx.xx.1:7001/console`.

6. Stop the AdminServer.

```
wls:/nm/mydomain> nmKill('AdminServer')
```

7. Exit the WebLogic Scripting Tool. Example:

```
exit()
```

8. SSH to the Essbase secondary node (Host 2), navigate to `<Domain_Home>/bin`, and run `startNodeManagerAdmin.sh` in the background. Example:

```
cd /u01/oracle/user_projects/domains/essbase_domain2/bin
./startNodeManagerAdmin.sh &
```

9. Set the domain environment. Example:

```
source /u01/oracle/user_projects/domains/essbase_domain2/bin/
setDomainEnv.sh
```

10. Run the WebLogic Scripting Tool, located in `<ORACLE_HOME>/oracle_common/common/bin`. Example:

```
/u01/oracle/user_projects/oracle_common/common/bin/wlst.sh
```

11. At the `wls:/offline>` prompt, connect to Node Manager, then start the AdminServer. For example, use the following commands (replace <*variables*> with your values):

```
wls:/offline>
nmConnect('<WebLogic_admin_user>','<WebLogic_admin_password>', '<Virtual-
IP-address>','9557','<DOMAIN_NAME>','<DOMAIN_HOME>','ssl')
wls:/nm/mydomain> nmStart('AdminServer')
```

Example:

```
wls:/offline> nmConnect('wladmin','wlpa55w0rD',
'<100.xx.xx.1>','9557','essbase_domain','/u01/oracle/user_projects/domains/
essbase_domain2','ssl')
wls:/nm/mydomain> nmStart('AdminServer')
```

12. Check that you can access the WebLogic Server Administrative console using the virtual IP address. For example, `http://100.xx.xx.1:7001/console`.

# Connection String Formats

Here are formats of connection strings used by relational databases that Essbase supports for configuring the RCU repository database.

These connection strings are useful when, while using the Essbase configuration tool, you get to the Database Connection screen.

The supported databases you can use for Essbase RCU schemas are listed in the Certification Matrix under Database.

**Oracle Database**

Here are examples of several supported connection string formats for specifying Oracle Database as the repository:

Syntax (PDB):

```
<host>:<port>/<PDB>
```

Example (PDB):

```
somedb99.example.com:1234/orclpdb
```

Syntax (SID):

```
<host>:<port>/<SID>
```

Example (SID):

```
somedb99.example.com:1234/ORCL
```

Syntax (Service_Name):

```
<host>:<port>/<service_name>
```

Example (Service_Name):

```
somedb99:1234/esscs.host1.oraclecloud.com
```

Syntax (Long service name):

```
(DESCRIPTION=(ADDRESS=(host=host_name)(protocol=protocol_name)
(port=port_number))
      (CONNECT_DATA=(SERVICE_NAME=service_name)))
```

Example (Long service_Name):

```
(DESCRIPTION=(ADDRESS=(host=oracle://somedb.example.com)(protocol=TCP)
(port=1521))
      (CONNECT_DATA=(SERVICE_NAME=orclpdb)))
```

**Microsoft SQL Server**

Here is an example of the connection string format for specifying Microsoft SQL Server as the repository:

In the example, `DBschema` (or `myDBschema`) is the name of the external source schema that contains tables and data.

Syntax:

```
<SQLServerHost>:<Port>:<DBschema>
```

Example:

```
MSSQLServerHost.example.com:1433:myDBschema
```

# Environment Locations in the Essbase Platform

Review common server locations related to the Essbase installation, including Oracle Home, application / domain locations, server and log file locations. Essbase does not set these locations as variables, but documentation references them frequently. Optionally, you can create aliases for these locations in your shell.

### Oracle Home

<*Oracle Home*> is the directory under which your Oracle products are hosted or installed.

When you're installing Essbase, it's installed to a pre-existing <*Oracle Home*>. It must be the same one that was set when you installed Fusion Middleware, which is a prerequisite to installing Essbase.

### Essbase Product Home

The directory under which Essbase software is hosted or installed. The value is always equivalent to `<Oracle Home>/essbase`.

### Domain Root

The location in which the Oracle WebLogic Server domain information and configuration artifacts are stored.

```
<Domain Root> = <Oracle Home>/domains
```

Example

```
/scratch/user/oracle_home/domains
```

To learn the value of your <*Domain Root*>, you can check the domain location value in `<Oracle Home>/domain-registry.xml`.

### Domain Name

The name of the Oracle WebLogic Server domain you specify during Essbase configuration.

`<Domain Name>` is created at the end of the `<Domain Root>` path.

### Example

```
essbase_domain
```

### Domain Home

The domain home is equivalent to `<Domain Root>/<Domain Name>`. Example:

```
<Oracle Home>/domains/essbase_domain
```

### Essbase Config Path

*<Essbase Config Path>* is an Essbase configuration directory. It should be in a separate location from the directory where Essbase software is installed (<*Essbase Product Home*>). Example:

```
<Domain Root>/<Domain Name>/config/fmwconfig/essconfig/essbase
```

*<Essbase Config Path>* is the location of the `essbase.cfg` configuration file. For information about its use, see Set Server-Level Configuration Properties.

### Essbase Path

*<Essbase Path>* is the directory of the Essbase Server. The value is typically equivalent to *<Oracle Home>*`/essbase/products/Essbase/EssbaseServer`.

### Application Directory

*<Application Directory>* is the full path you selected to store Essbase application artifacts. Formerly known as <*ARBORPATH*>, it is equivalent to:

```
<Oracle Home>/applications/essbase
```

In an environment set up for failover, the application directory must be a shared network mount accessible by both hosts.

Linux Example

```
/u01/essbase_data/applications/essbase
```

Windows Example

```
z:\essbase_mount\essbase_data\applications\essbase
```

When Essbase documentation refers to *the cube directory*, it means *<Application Directory>*`/app/`*<Application Name>*`/`*<Cube Name>*. For example, the cube artifacts for the cube named Basic within the application named ASOSamp are stored in the cube directory, which is *<Domain Root>*`/applications/essbase/app/ASOSamp/Basic`.

### ESS ES Home

*<ESS ES Home>* is a working folder for Essbase Java API configuration, buffering, and caching requirements. It is equivalent to:

```
<Domain Root>/<Domain Name>/config/fmwconfig/essconfig/aps
```

Select a separate location away from the directory where Java API and Provider Services software is installed (away from <*Essbase Product Home*>).

The Java API configuration file, `essbase.properties`, should be located in *<Ess ES Home>*`/bin`.

### EAS Home

*<EAS Home>* is the location of the optional managed server for Essbase Administration Services (EAS) Lite, if you configured it. The value is always equivalent to *<Essbase Product Home>*/products/Essbase/eas.

### Log Files

*<Log Home>* is the main directory for Essbase server logs. It is equivalent to:

*<Domain Home>*/servers/*<Essbase-Managed-Server-Name>*/logs

Example

*<Oracle Home>*/domains/essbase_domain/servers/essbase_server1/logs

Within *<Log Home>*,

- /aps/apsserver.log is the Provider Services log
- /essbase/platform.log is the Essbase platform log
- /essbase/jagent.log is the Essbase agent log
- /essbase/essbase/app/<application-name>/<application-name>_ODL.log is the Essbase application log

### See Also

Plan Your Essbase Environment

## Connect to Multiple Essbase 21c Servers in Shared Services and Administration Services

If your site uses multiple Essbase Server instances with Shared Services, you can access them all under one centralized Smart View URL. You can also administer all instances in on console using EAS Lite.

If needed for your site's configuration, you can:

- register multiple Essbase Servers within one Shared Services instance
- manage all Essbase Servers together in Essbase Administration Services (EAS Lite)

To configure and manage multiple Essbase Server instances with Shared Services identity provider, you will need to run the configuration tool for each Essbase Server, providing the same EPM_ORACLE_HOME and EPM_ORACLE_INSTANCE variables each time. Optionally, all Essbase Servers can share a centralized Smart View URL, and can be managed in EAS Lite.

> **Note:**
>
> The following applies only if you opt for the configuration to enable management of multiple Essbase Servers in one EPM Shared Services instance.
>
> - This configuration is supported only for independent deployments (not for Marketplace deployment on OCI).
> - Filter assignments and LCM operations are not supported from Shared Services Console.
> - After uninstalling an Essbase Server, you need to clean Essbase entries from the EPM registry. Otherwise, removed EssbaseCluster entries remain in Shared Services Console.

**Important:** Please read all steps before beginning. If you opt for configuring multiple Essbase Servers with a single Shared Services instance, it requires reconfiguration, and you cannot roll back the patch.

### Select a Workflow

To deploy multiple Essbase Servers that share one EPM Shared Services as the identity provider, select whichever of the following workflows is most appropriate for your circumstance.

1. Install Essbase 21c for the first time, as described in Install Oracle Essbase.
2. Stop Essbase services, as described in Stop, Start, and Check Servers.
3. If you are using a base installation of Essbase 21.1 or 21.2, use OPatch tool to upgrade to at least the 21.2.1.0.0 patch. For patching instructions, refer to Patch and Restore. If you are using 21.3 or higher, there is no need to apply a patch.
4. Run configuration to register multiple Essbase Servers with Shared Services and EAS Lite (instructions below).
5. Optionally, set up Essbase to access all Essbase Servers from one centralized Smart View URL, as described in Access Multiple Essbase Servers From Smart View.

**OR**

1. If you are using a base installation of Essbase 21.1 or 21.2, back up your existing applications. Refer to Back Up and Restore Essbase.
2. In addition to the backup, perform an LCM export of the applications so they can be re-imported after the reconfiguration. Refer to LcmExport CLI command (or Export LCM job).
3. Stop Essbase services as described in Stop, Start, and Check Servers.
4. If you are using a base installation of Essbase 21.1 or 21.2, use OPatch tool to apply the 21.2.1.0.0 patch. See Patch and Restore. If you are using 21.3 or higher, there is no need to apply a patch.
5. Run configuration to register multiple Essbase Servers with Shared Services and EAS Lite (instructions below).
6. Optionally, set up Essbase to access all Essbase Servers from one centralized Smart View URL. See Access Multiple Essbase Servers From Smart View.

### Register Multiple Essbase Servers with EPM Shared Services

To register multiple Essbase Servers with one instance of EPM Shared Services, perform these steps.

1. Follow steps 1-4 from your **Select a Workflow** path above (backing up applications, then installing or patching the software for each Essbase Server instance).
2. In your first Essbase Server installation, navigate to `<Oracle_Home>/essbase/bin` and run the configuration tool, `config.sh` (or `config.bat`). Refer to Configure Oracle Essbase for more information about the tool.
3. In the configuration page labeled Identity Provider, click **Enable EPM Shared Services Identity Provider**, and provide the path locations for your EPM system variables EPM_ORACLE_HOME and EPM_ORACLE_INSTANCE.
4. Optionally (also in the Identity Provider screen), provide a name for the Essbase Server you are registering with Shared Services. If you omit a name, the configuration will name it EssbaseCluster-1 (or EssbaseCluster-*n*).
5. Complete the remaining configuration tasks. As a result, the configuration registers your Essbase Server with Shared Services as EssbaseCluster-1 (or as the name you optionally provide). Note: This is a single Essbase Server, rather than an actual cluster.
6. Run configuration again for the second Essbase Server, providing the same EPM system locations you indicated for the first. As a result, the configuration registers the second Essbase Server with Shared Services as EssbaseCluster-2 (or as the name you optionally provide).
7. Continue to configure all additional Essbase Servers in the same way.
8. Re-import all of the applications, using the LcmImport CLI command (or Import LCM job).

**Notes**

- If you have registered multiple Essbase Server instances with Shared Services using Release 21.2.x or 21.3.x, and you want to rename them -- for example, if you want to create custom names to use instead of EssbaseCluster-1, EssbaseCluster-2, etc, then you must upgrade to Release 21.4 and reconfigure each instance using the Essbase deployment configuration tool, `config.sh` (or `config.bat`) in `<Oracle_Home>/essbase/bin`. In the Identity Provider screen of the configuration tool, you can select a custom name to register with Shared Services.
- Known Issue: In Shared Services Console, under Application Groups, if you double-click an application name under a de-registered EssbaseCluster, it returns a message `EPMLCM-13000: Service currently not available.`

### Register Multiple Essbase Servers with EAS Lite

You can manage all Essbase Server instances in a single EAS Lite console, as long as a) all the Essbase Server instances are registered with the same EPM Shared Services b) at least one of the Essbase Server instances has EAS Lite installed.

To register multiple Essbase Servers with one EAS Lite, perform these steps.

1. Follow steps 1-3 from your **Select a Workflow** path above (backing up applications, then installing or patching the software for each Essbase Server instance).
2. In at least one of your Essbase Server installations, navigate to `<Oracle_Home>/essbase/bin` and run the configuration as described in Configure Oracle Essbase.
3. In the configuration page labeled WebLogic Server Ports, select **Enable EAS**.

4. Complete the remaining configuration tasks. As a result, EAS Lite will be enabled for use with this Essbase Server.
5. Complete the instructions to access and use EAS Lite, as described in Use Essbase Administration Services Lite. The following limitations are removed when you use this configuration: inability to add, remove, and connect to additional Essbase Servers.
6. If you are using a secure Essbase port (HTTPS), see Add External Certificates to Essbase.
7. To add additional Essbase Servers to EAS Lite, see Adding Essbase Servers to Enterprise View.

   You must use the Discovery URL host specification format:

   ```
   https://wl_managed_server_host:wl_managed_server_port/essbase/agent
   ```

   where

   *wl_managed_server_host* is the WebLogic managed server host name of the Essbase Server.

   *wl_managed_server_port* is the WebLogic managed server port of the Essbase Server.

### Manual Steps to Clean EPM Registry

After uninstalling an Essbase Server, you need to clean Essbase entries from the EPM registry. Otherwise, removed EssbaseCluster entries will remain in Shared Services Console.

To clean the EPM registry, perform these steps.

1. Navigate to `<EPM_ORACLE_INSTANCE>/bin`.
2. List the components with type CLUSTER.

   ```
   ./epmsys_registry.sh view CLUSTER
   ```

3. Note the cluster IDs of your Essbase Server name (for example, EssbaseCluster-1), and the IDs of its children.
4. Delete the components with those IDs.

   ```
   ./epmsys_registry.sh deletecomponent \#componentID
   ```

5. For every child component of type APPLICATION, remove the corresponding file by replacing extensions `.ESB` or `.ESBAPP` with `.instance` in the ID.

   For example,

   Child ID: Sample_EssbaseCluster-1_1.ESBAPP

   Child ID: Analytic Servers:EssbaseCluster-1:1.ESB

   TYPE: APPLICATION

   ```
   ./epmsys_registry.sh removefile SYSTEM9/ESSBASE_PRODUCT/@'Analytic
   Servers:EssbaseCluster-1:1.instance'
   ```

   TYPE: APPLICATION

   ```
   ./epmsys_registry.sh removefile SYSTEM9/ESSBASE_PRODUCT/
   @'Sample_EssbaseCluster-1_1.instance'
   ```

6. List the components with type PROJECT.

```
./epmsys_registry.sh view PROJECT
```

7. Delete the components with those IDs.

```
./epmsys_registry.sh deletecomponent \#componentID
```

8. List the components with type PROVIDER_SERVICES_WEB_APP.

```
./epmsys_registry.sh view PROVIDER_SERVICES_WEB_APP
```

9. Note the ID of the component that has an **instance_home** and **localhost_name** matching your Essbase instance, and delete that component.
10. If Essbase Administration Services (EAS Lite) is configured, list the components with type ADMIN_SERVICES_WEB_APP.

```
./epmsys_registry.sh view ADMIN_SERVICES_WEB_APP
```

11. Note the ID of the component that has an **instance_home** and **localhost_name** matching your Essbase instance, and delete that component.

## Configure Microsoft SQL Server as Repository Database for Essbase Schemas

To use Microsoft SQL Server as the database for Essbase repository (RCU) schemas, you need to use case sensitive collation, and set READ_COMMITTED_SNAPSHOT to ON.

The following database configuration notes are applicable when you use Microsoft SQL Server as the database Essbase schemas, which include Metadata Services Schema (MDS), OPSS, and WebLogic (WLS) schemas.

- To create a metadata repository in SQL Server, set READ_COMMITTED_SNAPSHOT to ON for the hosting database. This enables the needed row versioning support. Use the following SQL command ALTER DATABASE, as in the following example:

```
ALTER DATABASE <DB NAME> SET READ_COMMITTED_SNAPSHOT ON
```

- Use case-sensitive collation to support the case-sensitive semantics in the metadata repository. For example, if Latin1_General is used, select the SQL_Latin1_General_CP1_CS_AS collation using the following SQL command:

```
DECLARE @collate sysname
SELECT @collate = convert(sysname,
serverproperty('COLLATION'))
IF ( charindex(N'_CI', @collate) > 0 )
BEGIN
select @collate = replace(@collate, N'_CI', N'_CS')
exec ('ALTER database <DB NAME> COLLATE ' + @collate)
END
GO
```

> **Note:**
>
> For both code sets above, you need to replace <DB NAME> with the actual name of your Essbase database.

In many cases, this command will run successfully. However, the command might fail and generate error messages concerning functions, primary keys, constraints, or indexes. This can be caused if the database already has collation aware objects. In this case, SQL Server does not allow you to change the collation at the database level. In this case, the alternative is to create a new database with the expected collation for MDS to use.

- There are some minor differences between an Oracle schema and a SQL Server schema. The length of the certain text fields are shorter for a SQL Server schema. For example, the full path name of the metadata in SQL Server is limited to 400 characters.
- Some WebCenter domain configurations do not require MDS schema, but all WebCenter domains require OPSS and WLS schemas.

See Configuring a Microsoft SQL Server Database for the Metadata Services (MDS) Schema.

5

# Select Identity Provider

For user authentication, you can choose WebLogic security in conjunction with your choice of external authentication identity provider, or, if you already use EPM Shared Services, you can continue to use it.

If you use EPM Shared Services, you must install and integrate Essbase On-Premise with a separate EPM instance where you have installed only Foundation Services. Please note that an existing EPM installation can't be reused. You can migrate users and application permissions between the two Foundation Services.

**Topics:**



## About Identity Providers

You have a choice of the following options for your Essbase user management and authentication identity provider.

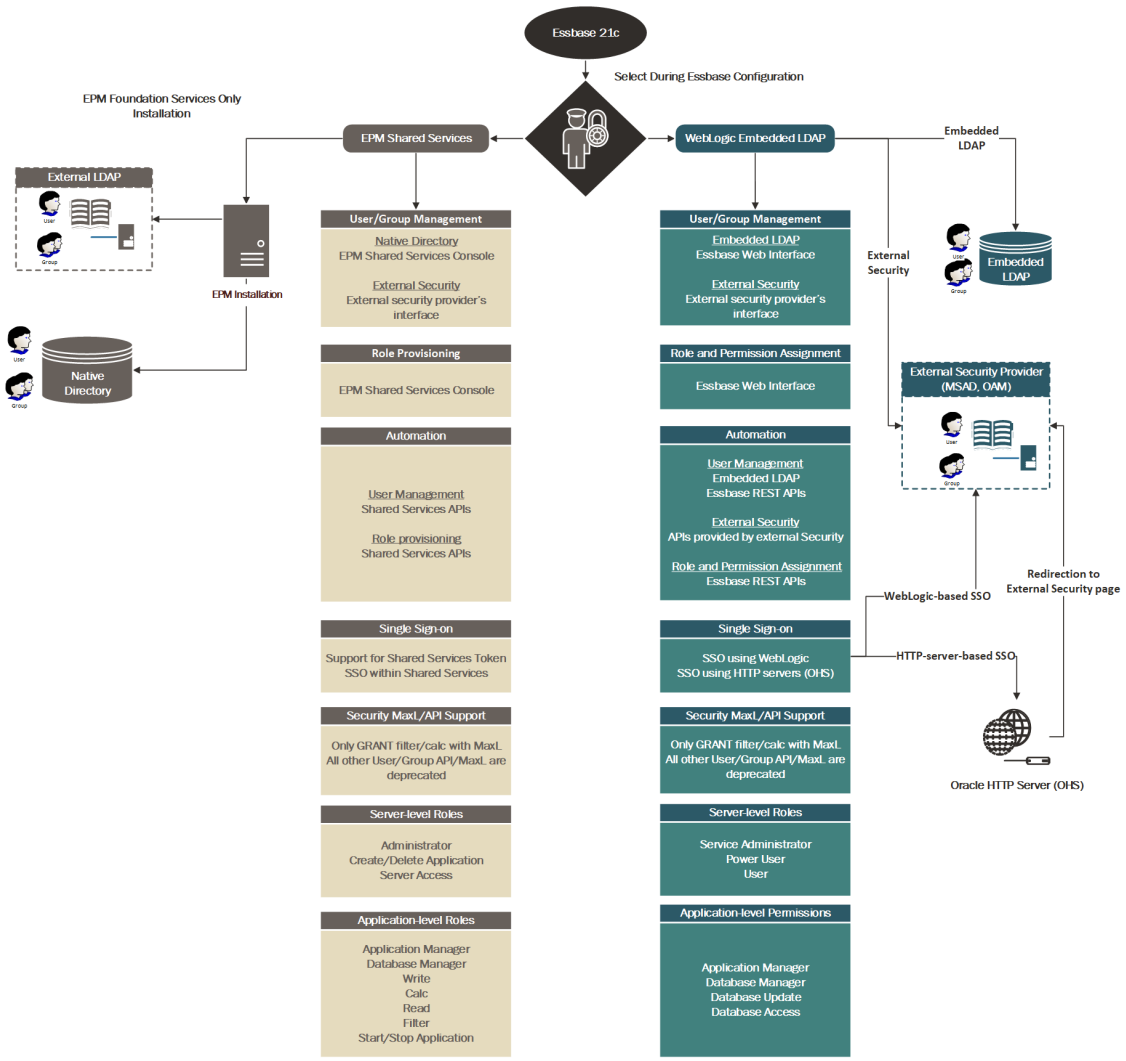
If you're currently an EPM customer and use Shared Services to manage your Essbase users, you can continue to do so. You cannot, however, integrate Essbase 21c directly into your existing EPM Foundation Services software. You must install a separate EPM Foundation Services [see the Compatibility Matrix for supported versions] and federate this new Shared Services instance with your LDAP provider. Application roles and any users/groups stored directly in Shared Services must be migrated to, and maintained in, the new Foundation Services. See EPM Shared Services Authentication.

If you don’t currently use Shared Services, or if you currently have only Essbase use cases, use the default WebLogic service provider. WebLogic can be federated with many external authentication identity providers. See WebLogic Authentication.

**Table 5-1 Provider Comparison**

| Identity Provider | Users and Groups | Assign User Role | Single Sign-On Support |
|---|---|---|---|
| • WebLogic Embedded LDAP (default).<br>• External LDAP or security provider. | • Users and groups are managed by WebLogic or external security provider.<br>• WebLogic Embedded LDAP - users and groups are created and managed using Essbase web interface or REST API.<br>• External LDAP/ identity providers - Users and groups are created and managed directly within the external provider. | Essbase web interface or Essbase REST API | Yes. It can be configured using WebLogic Administration Console. If you use Oracle HTTP Server, you can configure SSO using Oracle HTTP Server (OHS). |
| EPM Shared Services<br>• Built-in (native) LDAP (default)<br>• External LDAP/ identity provider | Users and groups are managed using Shared Services Console in the EPM installation. | Shared Services Console | No |

**Provider Options Diagram**




# WebLogic Authentication

Here are various options for configuring WebLogic authentication, which is the default mode. You can optionally use an external LDAP or identity provider.

If you're using WebLogic authentication, it's recommended to federate users to an external authentication provider, such as Microsoft Active Directory, which is suitable for large production environments. If you use WebLogic with the internal LDAP that is included with it, it is called "WebLogic Embedded LDAP." This configuration is not recommended for production use.

After you federate users to an external provider, native users remain in WebLogic, but only the WebLogic administrative user can log in to Essbase. Use the WebLogic administrative user to assign Essbase roles to federated users.

### Configure WebLogic to Use LDAP

You can integrate Essbase WebLogic with LDAP.

See Configuring Weblogic to use LDAP.

### Configure WebLogic to use Microsoft Active Directory

You can integrate Essbase WebLogic with Microsoft Active Directory (MSAD). Users and groups are then managed using MSAD administration tools, and user roles are assigned in the Essbase web interface or using REST APIs.

See Integrate WebLogic to Use Microsoft Active Directory.

### Configure WebLogic-based Single Sign-On

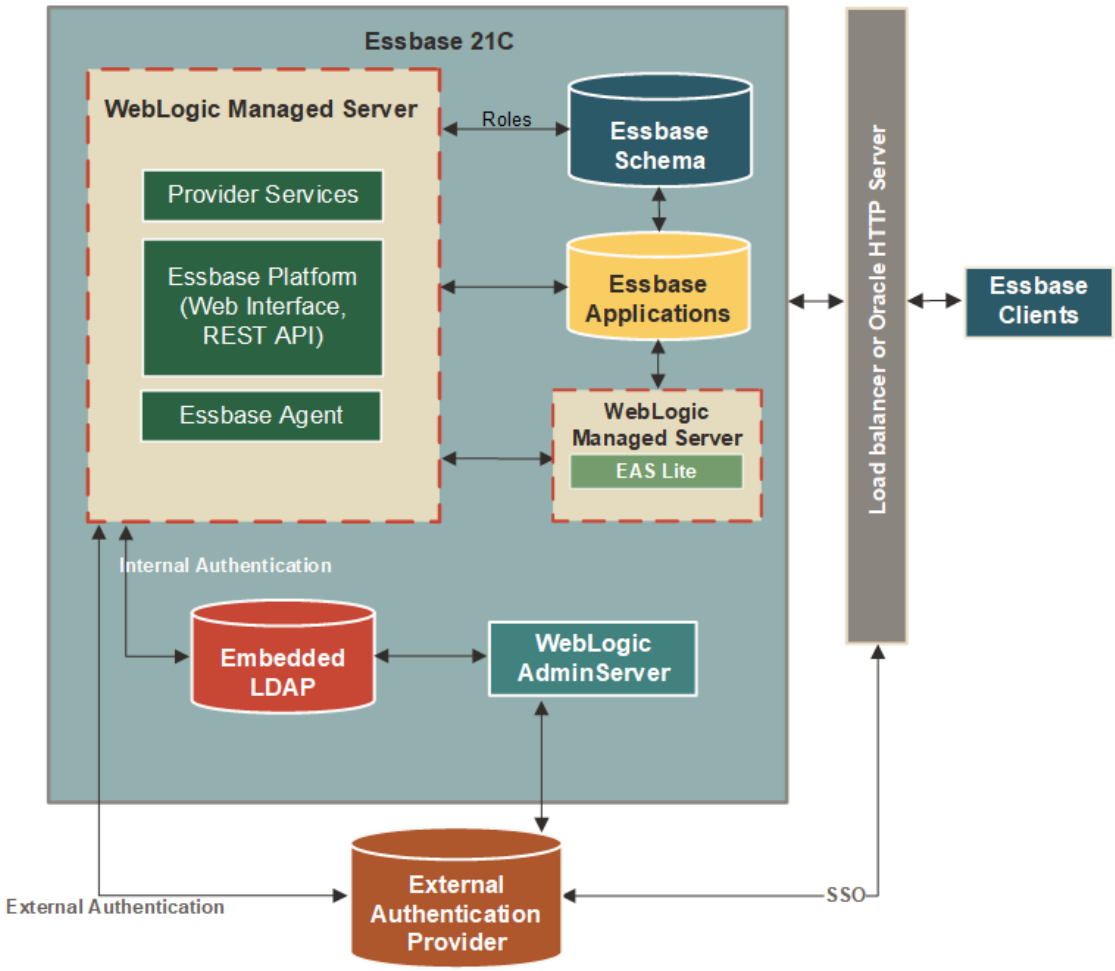
You can directly configure Essbase endpoint URLs within WebLogic to use Single Sign-On (SSO) - to add SSO support WebLogic endpoint URLs (with default port 9000). You can add and configure any external authentication provider in WebLogic Administration Console.

- See Single Sign-On Using Oracle Access Management Identity Federation Services
- See Single Sign-On Using MSAD Federation Services

### Configure Oracle HTTP Server-based SSO

If you use a load balancer or a web server, such as Oracle HTTP Server (OHS), you can also configure it to point to the same external security provider for SSO use cases. Note that this only addresses an SSO-based use case. You must still configure WebLogic to point to the external authentication provider.

### Essbase WebLogic Authentication Diagram




# Integrate WebLogic to Use Microsoft Active Directory

You can integrate Essbase WebLogic with Microsoft Active Directory (MSAD).

**Note:** If Active Directory is integrated through Identity and Access Management (IAM) or Oracle Identity Cloud Service (IDCS), then configure the Active Directory bridge as described in the links below:

For IAM, see Setting Up a Microsoft Active Directory Bridge

For IDCS, see Manage Microsoft Active Directory (AD) Bridges for Oracle Identity Cloud Service

### Add Provider

To add the Microsoft Active Directory provider to your security realm,

1. Log in to the WebLogic Server Administration Console for your Essbase instance.

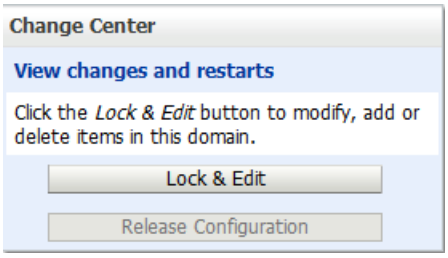
   To get to the console,

   a. In a browser, enter `<host_url>:<wl_adminserver_port>/console`, where `<host_url>` is http(s):// + the server name of your Essbase instance, and `<wl_adminserver_port>` is the Admin Server Port you specified in the **WebLogic Server Ports** screen during configuration.

For example, `http://myhost.example.com:7003/console`

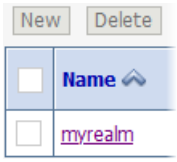
b. Log in as the WebLogic administrator account you specified in the **Domain Details** screen during configuration.

2. In the Change Center pane, click **Lock & Edit**.

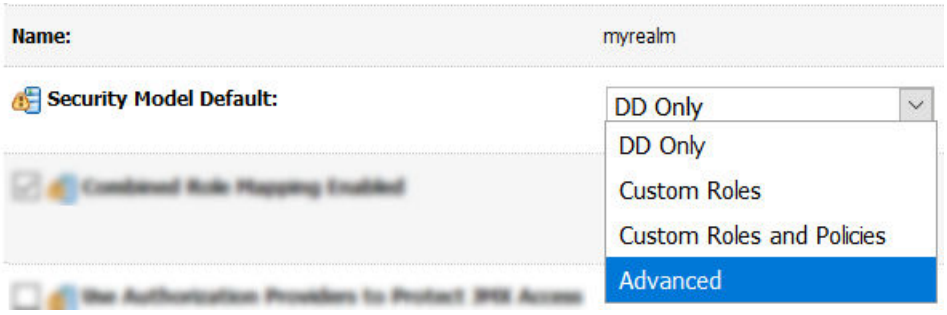



3. In the Domain Structure tree, under `<your domain name>`, click the **Security Realms** node.

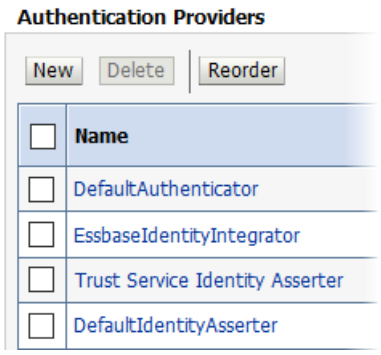

4. Click the name of the security realm so that you can open and configure it. For example, click the link **myrealm** (not the check box).



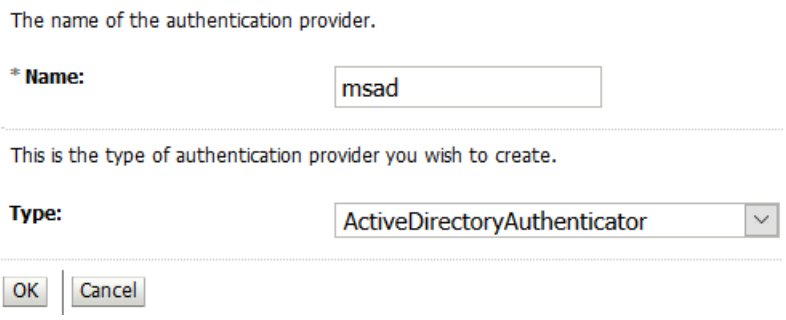

5. Modify **Security Model Default** from **DD Only** to **Advanced**, and click the **Save** button.



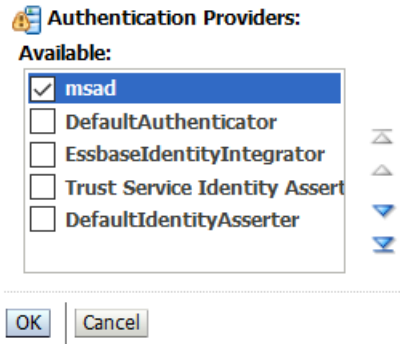

6. Select the Providers tab and click **New** to create a new authentication provider.



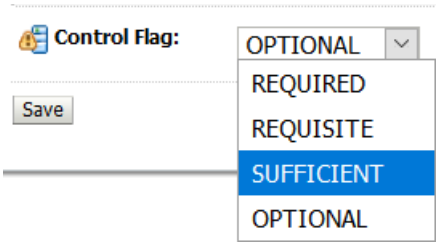

7. Enter **msad** as the name of the new authentication provider.



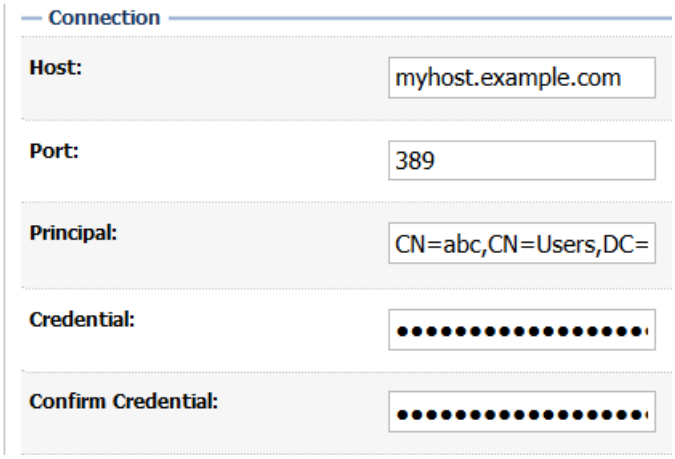

8. Select **ActiveDirectoryAuthenticator** as the authentication provider type, and click **OK**.
9. Click **Reorder**. Move the **msad** provider up, using the buttons, so that it's the first provider, and click **OK**.



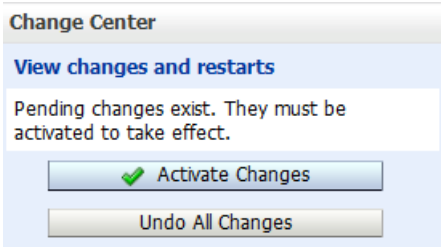

10. From the Authentication Providers list, click the link for the new provider (click the text link **msad**). In the settings, change the **Control Flag** from Optional to **Sufficient**, and click **Save**.




11. On the Provider Specific tab for the added **msad** provider, enter provider details.
    a. In the Connection section, enter your provider details for Host, Port (389), and Principal (you can save entering the credentials for last).




    b. In the Users section, enter your provider details for User Base DN.
    c. In the Groups section, enter your provider details for Group Base DN.
    d. In the Connection section, enter the Credentials twice: in Credential and Confirm Credential.
    e. Click **Save**.
12. Click **Activate Changes**.




13. Start, Stop and Restart Essbase.

### Verify External Users Were Added

Optionally, verify that the external users were added to your security realm.

1. Log in again to the WebLogic Server Administration Console for your Essbase instance.

2. Repeat steps 3 and 4 from the steps above (go to Security Realms > myrealm).
3. Click the Users and Groups tab.
4. Click **Customize this table**.
5. In the filter, specify **Filter by Column** as Name, and specify a Criteria by entering the first letter of a known user name in the external provider. Click **Apply**. The filtered list of users should appear in the table.

#### Assign Roles

After federation to an external authentication provider, WebLogic Embedded LDAP users can't log into Essbase. Only the WebLogic Administrator user remains.

As the WebLogic Administrator account, use the Service Role Provisioning REST API endpoint, PUT /essbase/rest/v1/permissions/{id}, to assign Essbase service administrator role to at least one federated user. Then, this new service administrator can provision other external users with Essbase roles, using either the Essbase web interface or the REST API.

For example, to provision Active Directory user “sysadmin” with service_administrator role, issue the REST request below, using cURL. Please replace `<weblogic_admin_user>`, `<weblogic_admin_password>`, `<Essbase_Host>`, `<Essbase_Managed_Server_Port>`, and `<sysadmin>` with appropriate values for your environment.

```
curl -k -X PUT -u <weblogic_admin_user>:<weblogic_admin_password> "http://
<Essbase_Host>:<Essbase_Managed_Server_Port>/essbase/rest/v1/permissions/
sysadmin" -H "accept: application/json" -H "Content-Type: application/json" -
d "{\"links\": [ {\"rel\": \"string\", \"href\": \"string\", \"method\":
\"string\", \"type\": \"string\" } ], \"id\": \"sysadmin\", \"name\":
\"sysadmin\", \"role\": \"service_administrator\", \"group\": false}"
```

## Single Sign-On Using MSAD Federation Services

You can enable Essbase to use single sign-on (SSO) from Microsoft Active Directory (MSAD) Federation Services (FS).

- You must integrate Essbase with MSAD according to the instructions in Integrate WebLogic to Use Microsoft Active Directory. Note that no explicit role assignment is necessary in this single sign-on topic, as it is already addressed in the pre-requisite WebLogic integration.
- You must make WebLogic Managed Server SSL-enabled, and only HTTPS URL can be protected. This task is included in the following steps.
- The following tasks, to enable Essbase to use Single Sign-On using MSAD Federation Services, must be performed in the order presented.

#### Part A - Launch Active Directory Federated Services (ADFS) and Download Federation Metadata XML

1. Connect to the Microsoft Windows system running ADFS and start the ADFS management interface. This provides SSO access for client computers. After launching, return to the source system.
2. From your Essbase local system, download the ADFS metadata, using the following sample link:

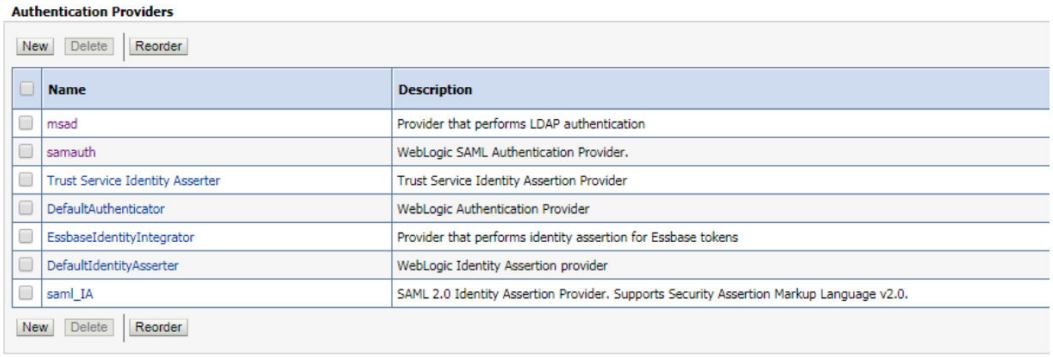
```
https://<ADFS_hostname>/federationmetadata/2007-06/federationmetadata.xml
```

This metadata is required for WebLogic integration with ADFS.

3. Edit `federationmetadata.xml` and remove the following tags, as they're not recognized by WebLogic. Delete the complete tags including the child tags.
   - `<ds:Signaturexmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ..... </X509Data></KeyInfo></ds:Signature>`
   - `<RoleDescriptor xsi:type="fed:ApplicationServiceType" ..... </EndpointReference></fed:PassiveRequestorEndpoint></RoleDescriptor>`
   - `<RoleDescriptor xsi:type="fed:SecurityTokenServiceType" ..... </EndpointReference></fed:PassiveRequestorEndpoint></RoleDescriptor>`
   - `<SPSSODescriptor WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"> ..... .... </SPSSODescriptor>`

**Part B - Configure Service Provider (SP) SSO**

1. Enable SSL:
   a. In WebLogic Administration console, go to myrealm > Providers Summary of Environment > Summary of Servers > essbase_server1 (setting page for your Essbase server.)
   b. In Configuration tab > General tab, select **SSL Listen Port Enabled** check box.
   c. Specify an SSL Listen port.
   d. Click **Save**.
   e. Go to Protocols > HTTP tab and specify Front end host, HTTP port, and HTTPS port details.
   f. Save and activate the changes.
2. Create an Identity Asserter:
   a. Go to Security Realms > myrealm > Providers.
   b. Select **Lock and edit**.
   c. Click **New** and create a new **SAML2IdentityAsserter**, such as `saml_IA`.
3. Create a new Authentication Provider:
   a. Enter a new provider by entering provider name, such as `samauth`.
   b. Select new provider type, such as SAMLAuthenticator, and click **OK**.
   c. Click the newly created provider, and select **Control Flag** value to change it to **SUFFICIENT**.
   d. Save the changes.
4. Under myrealm > Providers, reorder the providers. For example:




5. Click **All Changes** to activate and restart WebLogic admin and managed servers.
6. After WebLogic restarts, log in to WebLogic administration console, and go to Environment > Servers > essbase_server1 > Federation Services > SAML 2.0 Service Provider.
7. Click **Lock and Edit**.
8. Select **Enabled**.
9. Specify the default URL as

   ```
   https://<your-essbase-host>:<your Essbase SSL port>/essbase/jet/
   ```

   Ensure that **Preferred Binding** is set to **POST**, and click **Save**.
10. Under Servers > essbase_server1 Federation Services > SAML 2.0 General, specify the following details.
    a. Contact person details. When adding in ADFS, it shouldn't conflict with other registrations.
    b. Published site URL should be

       ```
       https://<Managed_server_host>:<Managed_Server_SSL_Port>/saml2
       ```

    c. Entity ID as `<wls_sp_for_adfs_hostname>`. Make sure to specify a unique name, when adding in ADFS, so it shouldn't conflict with other registrations.
11. Click **Activate changes**.
12. Click **Publish Metadata** and save the file it to a directory. You must register this file with ADFS. Copy the `spd.xml` file to the system where ADFS is located.
13. To register ADFS in WebLogic Server, copy the file downloaded `federationmetadata.xml` (generated in STEP A) from ADFS machine to WebLogic Server machine. It must be accessible to WebLogic AdminServer, for example: `/scratch/user/federationmetadata.xml`.
14. Go to Security Realms myrealm Providers > Authentication > saml_IA Management > New > New Web Single Sign-On Identity Provider Partner.
15. Click **WebSSO-IdP-Partner-0** and enter the following:
    a. Description: enter the same value as for name.

b. Enter Redirect URIs:

```
/essbase/jet/*
/essbase/smartview
/essbase/smartview/*
/essbase/smartview*
/essbase/ui
```

16. Edit `./Oracle/domains/esscs/bin/setDomainEnv.sh` and add `-DLOGOUT_URL` to the JVM arg `EXTRA_JAVA_PROPERTIES: EXTRA_JAVA_PROPERTIES="<Extra_Java_Properties> -DLOGOUT_URL=https://MSAD-Host/adfs/ls/?wa=wsignout1.0" export <Extra_Java_Properties>`

> **Caution:**
>
> The Essbase platform includes scripts in `<DOMAIN HOME>/bin` that can customize the environment and behaviors of Essbase functionality. However, making changes to these domain environment or startup scripts can have unintended effects, including startup failure. Oracle recommends making changes in a test environment first. Before editing these scripts, always:
>
> a. Stop the Essbase managed servers, using `<DOMAIN HOME>/esstools/bin/stop.sh` (on Linux), or `<DOMAIN HOME>\esstools\bin\stop.cmd`(on Windows).
>
> b. In `<DOMAIN HOME>/bin`, make a backup copy of the file you want to edit. For example,
>
> On Linux
>
> ```
> cp setStartupEnv.sh setStartupEnv_bak.sh
> ```
>
> On Windows
>
> ```
> copy setStartupEnv.cmd setStartupEnv_bak.cmd
> ```
>
> c. Edit carefully, using only Oracle's documented instructions, or working with Oracle Support.
>
> d. Restart Essbase, using `<DOMAIN HOME>/esstools/bin/start.sh` (on Linux), or `<DOMAIN HOME>\esstools\bin\start.cmd`(on Windows). Check that startup completed normally.

17. Restart the WebLogic AdminServer and managed servers after activating the changes.

**Part C - Configure ADFS IDP**

1. Go to the ADFS system where ADFS Management interface is running. Under Trust Relationships > Relying Party Trusts, right-click, and launch **Add Relying Party Trust....**
2. Click **Start**.
3. In the **Import data about the relying party from a file** option, browse to the Federation metadata file location spd.xml for download from WebLogic and click **Next**.
4. Specify a display name and click **Next**.

5. Select **I do not want to configure multi-factor...**, and click **Next**.
6. Accept the default option, and click **Next**.
7. Select **Open the Edit Claim Rules dialog...** check box.
8. In Edit Claim Rules dialog, click **Add Rule**.
9. Select rule template **Send LDAP Attributes as Claims**.
10. Enter the following:
    a. Enter **Claim rule name**: `Name`.
    b. Select **Attribute store**: `Active Directory`.
    c. Under **LDAP Attribute**, select `SAM-Account-Name`.
    d. Under **Outgoing Claim type**, select `Name ID`.
11. Click **Finish**.
12. Similarly, add another rule, Claim rule name: GivenName; Attribute store: Active Directory; Under LDAP Attribute, select **Given-Name**; and under Outgoing Claim type, select **Given Name**; and click **Finish**.
13. Click **Apply** in the Edit Claim Rules dialog, and close it.
14. Double-click the newly added Relaying Party Trust, and go to Advanced tab. Select the Secure hash algorithm: `SHA-1`.
15. Click Endpoints > Add SAML, and enter the details shown below.
    a. **Endpoint type**: SAML Logout
    b. **Binding**: POST
    c. **Trusted URL**: (in the format of:) `https://host:port/adfs/ls/?wa=wsignout1.0`
16. Record the Entity ID you entered in **Part B - Configure Service Provider (SP) SSO** above, step 10c. Then open power shell and run the command:

```
set-AdfsRelyingPartyTrust -targetIdentifier <Entity ID> -
SigningCertificateRevocationCheck None -
EncryptionCertificateRevocationCheck None
```

The setup is now completed.

### Part D - Test MSAD FS Single Sign-On

1. Launch Essbase at the HTTPS URL, such as https://host:port/essbase/jet.
2. You should see MSAD user at the top right corner of the Essbase user interface.

> **Note:**
>
> If, after logout, the browser session is closed (deleted), then restart the browser to log in as a different user.

# Single Sign-On Using Oracle Access Management Identity Federation Services

You can enable Essbase On-Premise to use single sign-on (SSO) from Oracle Access Management Identity Federation Services (FS). This describes how to configure Oracle Access Management Identity Federation as an Identity Provider (IDP) to be used with WebLogic as the Service Provider (SP).

- You must have an Oracle Access Manager (OAM) environment with Federation Services enabled. OAM is integrated with an LDAP directory, such as OUD, OID, or AD. Here, OID is integrated with OAM.
- You must have Essbase installed.
- The following tasks, to enable Essbase to use Single Sign-On using Oracle Access Management Identity Federation Services, must be performed in the order presented.

**PART A - Obtain the IDP metadata for SP configuration**

1. Log in to the OAM console and navigate to Configuration > Available Services.
2. Confirm that Identity Federation is enabled, or enable it.
3. Go to Configuration > Settings > View > Federation.
4. Click **Export SAML 2.0 Metadata** to download IDP metadata.
5. Save metadata file as `oam_fed_idp_metadata.xml` to use this file to register OAM as IDP in WebLogic.
6. Edit `oam_fed_idp_metadata.xml`, remove `<md:RoleDescriptor ... </md:RoleDescriptor` tag, and save the file. This tag isn't supported by WebLogic.

**PART B - Configure WebLogic service provider (SP)**

1. Enable SSL.
   a. In WebLogic console, under domain structure, go to Environment > Servers > essbase_server1 > configuration > General. Select **Listen Port Enabled** check box and provide a port number for Managed Server.
   b. Enable SSL for Protocol HTTP on Managed server. Under domain structure, go to Environment > Servers > essbase_server1 Protocol > HTTP. Select **SSL Listen Port Enabled** check box and provide a port number.
   c. Go to Security Realms > myrealm > Configuration > general Tab. Set **Security Model** to **Advanced**.
2. Create an Identity Asserter using WebLogic Admin console.
   a. Log in to WebLogic console.
   b. Go to Home > Summary of Security realms > myrealm > Providers.
   c. Click **Create a New Authentication Provider**.
   d. Click **OK**.
   e. Enter the provider name as `SAML-IA` and select type **SAML2IdentityAsserter**.
   f. Click **OK**.
3. Create a new SAMLAuthenticator provider.

a. Go to: Home > Summary of Security realms > myrealm > Providers.

b. Click **Create a New Authentication Provider**.

c. Click **OK**.

d. Enter the provider name as `SAML-auth` and select type **SAMLAuthenticator**.

e. Click **OK**.

4. Change **Control Flag** value to **SUFFICIENT** for authenticator created in above step.

a. Go to: Home > Summary of Security realms > myrealm > Providers > SAML-auth.

b. Under Configuration > Common, set the **Control Flag** to **SUFFICIENT**.

c. Click **Save**.

5. Create a new oid-auth provider.

a. Go to: Home > Summary of Security realms > myrealm > Providers.

b. Click **Create a New Authentication Provider**.

c. Click **OK**.

d. Enter the provider name as oid-auth and select type **OracleInternetDirectoryAuthenticator**.

e. Click **OK**.

f. Change **Control Flag** to **SUFFICIENT** for the oid-auth Provider added and click **Save**.

6. Select the Provider Specific tab and enter your OID server details. Take OID server details from OAM console > User Identity Store section.

a. From OAM Console configuration > User Identity Store, click **OID store**.

b. In Provider Specific section of oid-auth Provider, update the following sections with appropriate values.

- Connection section:
  - Enter Host: hostname of OID server
  - Principal: cn=orcladmin,cn=users,dc=us,dc=oracle,dc=com
  - Credential Confirm Credential: provide the credentials
- Users: User Base DN: cn=users,dc=us,dc=oracle,dc=com
- Groups: Group Base DN: cn=groups,dc=us,dc=oracle,dc=com
- Use Retrieved User Name as Principal: check

c. Accept the other fields' default values, and save all changes.

7. Enable Federation for managed server.

a. Go to Home > Environment Servers > essbase_server1 > configuration > Federation Services.

b. In SAML 2.0 Service Provider tab, select **Enabled** option and provide **Default URL** as

```
https://Essbase-Host:Essbase-Managed Server-SSL-Port/essbase/jet
```

Accept the remaining fields as default and save.

c. Obtain the SP metadata for IDP configuration: In SAML 2.0 General tab, provide appropriate values and save.

d. Once changes are saved, export SP metadata into an XML file, such as: `sp_metadata.xml`.

e. Click **Publish Meta Data**.

8. Create IDP partner on WebLogic using oam_fed_idp_metadata.xml file, copied from OAM box.

   a. Go to Security Realms > myrealm > Providers > Authentication > saml_IA > Management > New > New Web Single Sign-On Identity Provider Partner, such as: WebSSO-IdP-Partner-oam.

   b. Select `oam_fed_idp_metadata.xml file` and click **OK**.

   c. To enable IDP partner, click **WebSSO-IdP-Partner-oam**. select **Enabled** check box, and provide redirect urls.

9. Configure IDP on OAM console.

   a. Go to Federation > Identity Provider Management.

   b. Click **Create Service Provider Partner**.

   c. Enter the name.

   d. Ensure **Enable Partner** is selected.

   e. Accept SAML 2.0 as the protocol (default).

   f. Select metadata file downloaded from WebLogic (SP).

   g. Specify **NameID Format Settings**.

   h. Select **Unspecified** as the NameID format.

   i. Select **User ID Store Attribute** as the NameID Value.

   j. Enter User Attribute in the LDAP user record containing the user's identifier. Oracle Internet Directory is the User Data Store, the attribute is `uid`.

10. Edit `$ORACLE_HOME/user_projects/domains/Essbase-Domain/bin/setDomainEnv.sh` and add `-DLOGOUT_URL to the JVM arg EXTRA_JAVA_PROPERTIES` as shown below:
    Before the change:

```
EXTRA_JAVA_PROPERTIES="-
Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.WLSMB
eanServerBuilder ${EXTRA_JAVA_PROPERTIES}"
```

    After the change:

```
EXTRA_JAVA_PROPERTIES="-
Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.WLSMB
eanServerBuilder -DLOGOUT_URL=http://OAM-Host:OAM-Port/oam/server/logout $
{EXTRA_JAVA_PROPERTIES}"
```

**PART C - Assign roles**

After OID integration, embedded LDAP users, such as WebLogic, can't log into Essbase interface. Only REST/MaxL operations are allowed. Use embedded LDAP admin user to assign Essbase roles to OID users using REST. OID users can log into Essbase only after role assignment.

Once a role is assigned to at least one OID user (admin), that OID user can log into Essbase and assign roles to other users directly through the interface.

REST-based assignment example as shown here: `curl --insecure -X PUT -u weblogic:samplepass "http://host:9000/essbase/rest/v1/permissions/user1" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"links\": [ { \"rel\": \"string\", \"href\": \"string\", \"method\": \"string\", \"type\": \"string\" } ], \"id\": \"user1\", \"name\": \"user1\", \"role\": \"service_administrator\", \"group\": false}"`

**Part D: Test OAM FS Single Sign-On**

Open Essbase and run

`https://<essbase_vm>:<sslportno>/essbase/jet`

The request is redirected to OAM Federation login page.

> **Note:**
>
> If there is a logout issue, then in order to complete the logout action, close the browser.

# EPM Shared Services Authentication

If you use EPM Shared Services authentication with Essbase 21c, Shared Services manages all the Essbase users, groups, roles, and permissions.

**Requirements to Integrate EPM Shared Services with Essbase 21c**

Essbase 21c with Shared Services authentication requires a network-accessible, dedicated EPM 11g Services installation, separate from any EPM installation you have already deployed. Oracle recommends that this Foundation Services instance not be on the same host where you are running Essbase.

For versions prior to Essbase 21.2.1, you must install or reuse an existing EPM 11.1.2.4 or 11.2.x (Foundation only) and not use your existing Shared Services for Essbase integration. For versions of Essbase v21.2.1 and later, install EPM 11.2.x (including 11.2.x Essbase), to configure with 21.2.x.

> **Caution:**
>
> For versions prior to Essbase 21.2.1, if you attempt to configure Essbase with a production Essbase 11g instance that is associated with Essbase 11g On-Premise, your Essbase 11g instance in Shared Services will be overwritten!

If you plan to set up a failover environment, and you are using EPM Shared Services for authentication, then you must install EPM 11g Services to a shared network location accessible by all the Essbase nodes. If this is not possible, you can install only the EPM Foundation component locally in each Essbase node, but pointing to the same EPM Schema. Each Essbase node must be able to find the EPM_ORACLE_HOME and EPM_ORACLE_INSTANCE locations associated with your EPM installation.

**About User Directories**

User directories (also called identity providers, security providers, or external authentication providers), are directory services providing user and group authentication. LDAP is one example. By default, Shared Services uses a native LDAP directory to store users and groups, but you can optionally configure it to use a federated (external) LDAP or identity provider. To add an external provider to Shared Services, see Configuring LDAP Based User Directories.

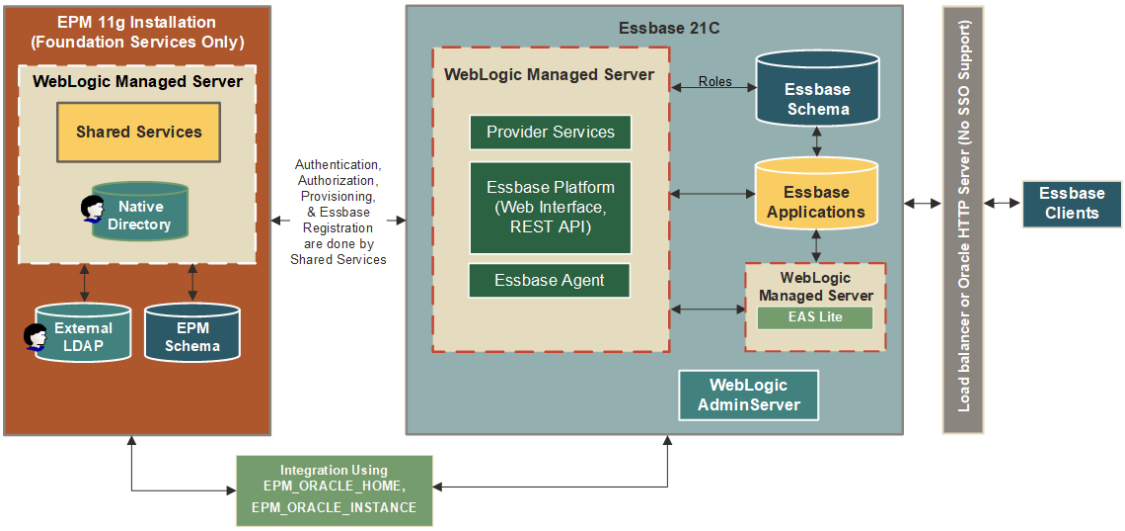
You can share one user directory between both EPM 11g Services instances.

**Configure Essbase with EPM Shared Services**

1. For versions prior to Essbase 21.2.1, you must install or reuse an existing EPM 11.1.2.4 or 11.2.x (Foundation only) and not use your existing Shared Services for Essbase integration. For versions of Essbase v21.2.1 and later, install EPM 11.2.x (including 11.2.x Essbase), to configure with 21.2.x.
2. Start Shared Services (it must be running when you go to configure Essbase).
3. Install Essbase 21.3 on the same system (or network) where you just installed EPM Services.
4. Configure Essbase. When you get to the Identity Provider screen,
    a. Click the check box to **Enable EPM Shared Services Identity Provider**.
    b. Specify the EPM installation locations <EPM_Oracle_Home> and <EPM_Oracle_Instance>. These EPM directories must be network-accessible from the Essbase 21c instance you are configuring. **All external providers configured in Shared Services for use by Essbase MUST have trust enabled.** See *Essbase 21 Not Authenticating to External Provider When Configured with Shared Services, Essbase UI Login Screen Flashes.* Doc ID 2938405.1*)*.
5. Complete the Essbase 21c configuration.
6. Choose an option:
    a. Federate the new Shared Services environment with your identity provider.
    b. Migrate users and groups only, using Shared Services. Do not select to export roles. Instead, use the 11g Export Utility or LCM Export to export roles with the application export.

    For more about these options, see Scenario 1 in Migrate Essbase 11g Users and Groups.
7. Migrate roles when you migrate applications. See Prepare to Migrate From Essbase 11g.

**Essbase and Shared Services Authentication Diagram**


EPM 11g Installation
(Foundation Services Only)
WebLogic Managed Server
Shared Services
Native Directory
External LDAP
EPM Schema
Authentication, Authorization, Provisioning, & Essbase Registration are done by Shared Services
Essbase 21C
WebLogic Managed Server
Provider Services
Essbase Platform (Web Interface, REST API)
Essbase Agent
Roles
Essbase Schema
Essbase Applications
WebLogic Managed Server
EAS Lite
WebLogic AdminServer
Load balancer or Oracle HTTP Server (No SSO Support)
Essbase Clients
Integration Using EPM_ORACLE_HOME, EPM_ORACLE_INSTANCE

6

# Secure Your Communication and Network

Your can secure your communication and network, with secure encryption using TLS Everywhere, certificates, single sign-on, and more.

**Topics:**



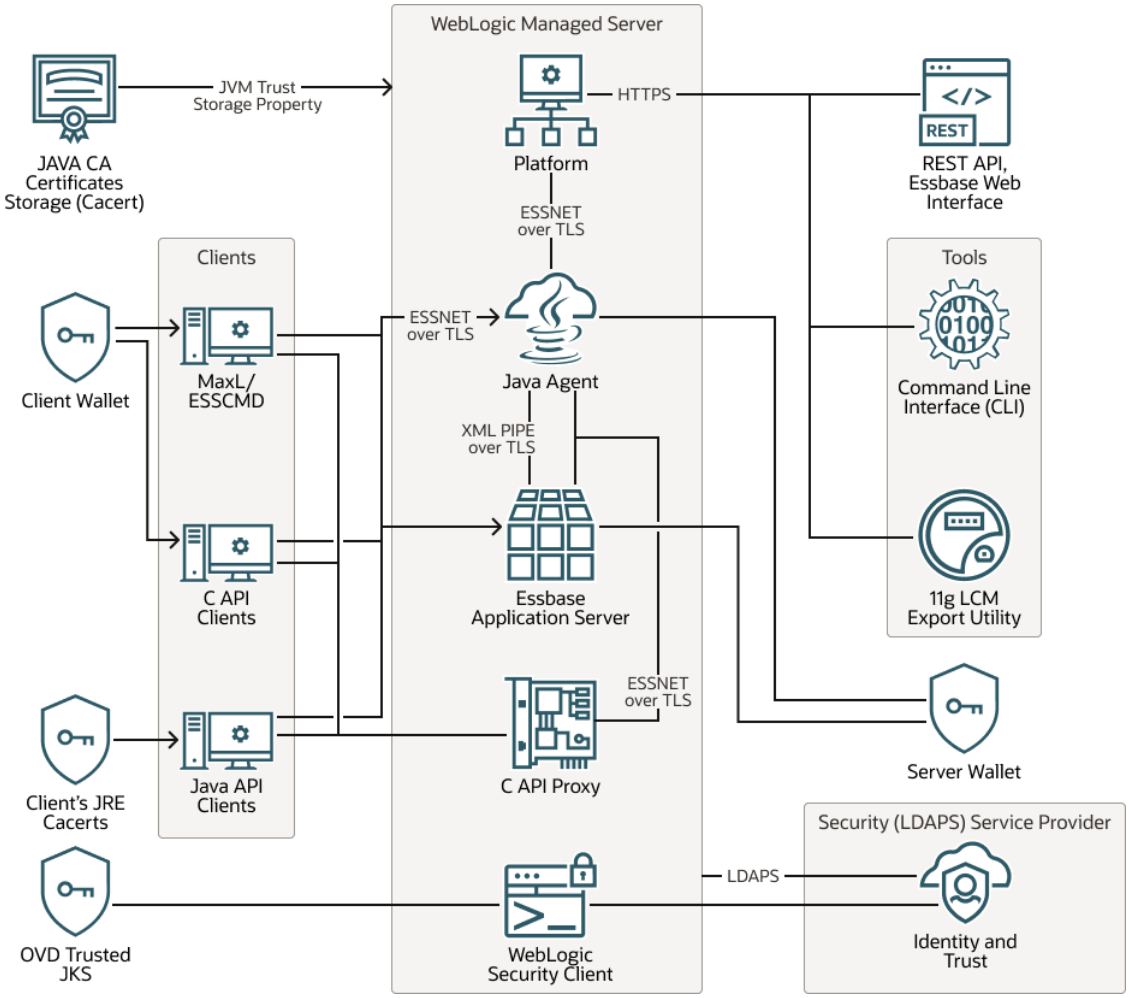
## About Securing Your Communication and Network

Transport Layer Security (TLS) and its deprecated predecessor, Secure Sockets Layer (SSL) are cryptographic protocols designed to provide communications security over a computer network. TLS works in much the same way as SSL, using encryption to protect the transfer of data and information.

In general, authentication certificates include those signed by a certification authority (CA), or self-signed certificate (which requires additional configuration so that the client software "trusts" it).

TLS can be enabled during Essbase deployment configuration, or after Essbase configuration.

**TLS Everywhere Secure Communication Topology and Components**
The diagram below shows components and interfaces that are secured by TLS communication encryption. Essbase configuration includes the option of enabling TLS security configuration.




**Security certificate storage used in the system:**

- JAVA CA Certificates Storage - stores all CA certificates, including self-signed ones (found using the Java Virtual Machine (JVM) trust store)
- Client Wallet - storage used by C API clients for trusted certificates only; uses TSSNET protocol
- Client's JRE Cacerts - cacerts file located inside JAVA runtime, contains all keys that this running JAVA instance will trust. This is an Essbase client in this runtime.
- OVD Trusted JKS (Oracle Virtual Directory Trusted Java Key Storage) for trusted certificates for LDAP over TLS (LDAPS)
- Platform - Oracle Platform Security Services (OPSS) - identity and trust storage for WebLogic for WebLogic certificates
- Server Wallet - storage for both trusted and identity certificates, used by Essbase application servers (ESSSVR)

**Clients:**

- MaxL (administrative scripting language) / ESSCMD (old Essbase command language)
- C API Clients - custom C API clients
- Java API Clients - trusted Java key storage (JKS) for client-trusted certificates

**WebLogic Managed Server:**

- Platform - web service that provides access to database features, including REST API and Essbase web interface
- Java Agent - Essbase Java Agent (JAgent), instance as a service that manages Essbase applications and security; controls start/stop of every application; controls access of various clients to applications; Platform is used in Java Agent as requested
- Essbase Applications Server - service that performs different tasks regarding storing, calculating, activating data; it's a multidimensional analytic engine that performs all operations - all other components of this system are built only to provide access to this engine
- C API Proxy - proxy service that can provide access directly to Java Agent and Essbase Applications Server; makes possible to connect to internal ESSNET services inside HTTP protocol; every client that supports this API proxy can work directly with Java Agent and Essbase Applications Server
- WebLogic Security Client - service that you can configure for Java Agent and Platform to work as a bridge between different security services providers and all components in the system; uses LDAP protocol

**Interfaces and Tools:**

- REST API and Essbase web interface
- Essbase Command-line Interface tool (CLI)
- 11g LCM Export Utility for migration

**Security (LDAPS) Service Provider** - can provide security services - indication and authentication (identity and trust) and also used for secure storage for identify and certificates

**Protocols by which communication between components are secured:**

- HTTPS
- ESSNET over TLS - Essbase proprietary networking protocol
- XML PIPE over TLS
- LDAPS

# Use Cases for Securing Independent Deployments

Here's some use cases for securing your communication and network for independent deployments.

**Use Cases - for Independent Deployments**

- Set up Weblogic TLS connection for Essbase
- Update TLS Certificates for Essbase 21c configurations
- Add External Certificates to Essbase
- Add external certificates for external Java process (for example, JAPI). If you use a self-signed certificate and a Java client, you must configure your Java client - See the Steps for Using Java-based Clients with Self-Signed Certificates in Add External Certificates for External Java Process.
- Replace Self-Signed Certificates with CA Certificates
- Configure TLS for Essbase Failover - You can also configure TLS for Essbase failover to work with secure mode.

# Set up Weblogic TLS Connection for Essbase

By default, WebLogic is configured in unencrypted mode. Here are the steps to add a WebLogic TLS connection to the existing unsecured domain.

**Set up TLS connection for Essbase 21.2 or 21.3+**

> **Note:**
>
> Prerequisites and notes for updating JAgent and WebLogic certificates.
>
> - Set Oracle Home environment variables - point to Essbase installation. JAVA_HOME and ORACLE_HOME environment variables must be defined to run configuration.
> - The parameter of command file is the response file location (this file is generated in GUI mode and is used in silent mode) or DOMAIN_HOME location.

1. Stop Essbase
   For Linux:

   ```
   ${DOMAIN_HOME}/esstools/bin/stop.sh
   ```

   For Windows:

   ```
   %DOMAIN_HOME%\esstools\bin\stop.cmd
   ```

2. To update all TLS certificates (configured in Essbase 21.2 or 21.3+) and the wallet, run the following:

   > **Note:**
   >
   > RESPONSE_FILE and DOMAIN_HOME cannot both be used together in script parameters. Only use one of them.

   For 21.2 or 21.3+ on Linux:

   ```
   java -cp $ORACLE_HOME/essbase/lib/essbaseconfig.jar
   com.oracle.wizard.operation.helper.ssl.SslConfigHelper
   [RESPONSE_FILE=<response file> | DOMAIN_HOME=<${DOMAIN_HOME}>]
   ```

> **Note:**
>
> For 21.3+ on Linux, you can also use the following command (this does not require export JAVA_HOME and ORACLE_HOME):
>
> ```
> ${ORACLE_HOME}/essbase/bin/ssl_config.sh [RESPONSE_FILE=<response
> file> | DOMAIN_HOME=<${DOMAIN_HOME}>]
> ```

For 21.3+ on Windows:

```
java -cp %ORACLE_HOME%\essbase\lib\essbaseconfig.jar
com.oracle.wizard.operation.helper.ssl.SslConfigHelper
[RESPONSE_FILE=<response file> | DOMAIN_HOME=<%DOMAIN_HOME%>]
```

> **Note:**
>
> You can also use the following command:
>
> ```
> %ORACLE_HOME%\essbase\bin\ssl_config.cmd [RESPONSE_FILE=<response
> file> | DOMAIN_HOME=<%DOMAIN_HOME%>]
> ```

3. Since passwords of wallet and keystores are not changed, just run WebLogic to start Essbase. Start Essbase. See Stop, Start, and Check Servers.
   For Linux:

   ```
   ${DOMAIN_HOME}/esstools/bin/start.sh
   ```

   For Windows:

   ```
   %DOMAIN_HOME%\esstools\bin\start.cmd
   ```

**Set up SSL enabled mode for Essbase 21.2 or 21.3+**

If Essbase was configured in 21.1 version in encrypted mode, then after patching to Essbase 21.2 or 21.3+, you need to set up ssl enabled mode, using the following steps.

1. Call wlst.
   For Linux:

   ```
   ${ORACLE_HOME}/oracle_common/common//bin/wlst.sh
   ${ORACLE_HOME}/essbase/modules/oracle.essbase.sysman/scripts/
   ssl_settings.py
   ${DOMAIN_HOME} ${DOMAIN_HOME}/security/keystore.jks
   ${DOMAIN_HOME}/config/fmwconfig/ovd/default/keystores/adapters.jks
   ${DOMAIN_HOME}/config/fmwconfig/essconfig/essbase/walletssl/certwallet.pem
   <FQDN> <ssl Admin
   Port> <<EOF
   Password1
   ```

```
Password1
EOF
```

- For 21.2, instead of the Fully Qualified Domain Name <FQDN>, use:

  ```
  https://<FQDN>:<Essbase Server SSL Port>/essbase/agent
  ```

- For 21.3+, it should be pure FQDN host.

For Windows:

```
%ORACLE_HOME%\oracle_common\common\bin\wlst.cmd
%ORACLE_HOME%\essbase\modules\oracle.essbase.sysman\scripts\ssl_settings.py
%ORACLE_HOME%\security\keystore.jks
%ORACLE_HOME%\config\fmwconfig\ovd\default\keystores\adapters.jks
%ORACLE_HOME%\config\fmwconfig\essconfig\essbase\walletssl\certwallet.pem
<FQDN> <ssl Admin
Port>
```

The above command will prompt you to enter Password.

2. Change the following:
   For Linux: edit `${DOMAIN_HOME}/bin/setStartupEnv.sh`. Find the substring - Djavax.net.ssl.trustStore and change this line up until the end of the line (expand `${DOMAIN_HOME}`)

   ```
   -Djavax.net.ssl.trustStore=${DOMAIN_HOME}/config/fmwconfig/essconfig/
   essbase/walletssl/cacerts -
   Dweblogic.security.SSL.ignoreHostnameVerification=true
   ```

   For Windows: edit `%ORACLE_HOME%\bin\setStartupEnv.cmd`. Find the substring - Djavax.net.ssl.trustStore and change this line up until the end of the line (expand `%DOMAIN_HOME%`)

   ```
   -Djavax.net.ssl.trustStore=%ORACLE_HOME%
   \config\fmwconfig\essconfig\essbase\walletssl\cacerts -
   Dweblogic.security.SSL.ignoreHostnameVerification=true
   ```

3. Change the following:
   For Linux: edit `${DOMAIN_HOME}/bin/setWlstEnv.sh` as follows: (expand ${DOMAIN_HOME})

   ```
   export WLST_PROPERTIES="-Dweblogic.ssl.JSSEEnabled=true
   -Dweblogic.security.SSL.enableJSSE=true
   -Dweblogic.security.SSL.ignoreHostnameVerification=true
   -Dweblogic.security.CustomTrustKeyStoreType=JKS
   -Dweblogic.security.TrustKeyStore=CustomTrust
   -Dweblogic.security.CustomTrustKeyStoreFileName=${DOMAIN_HOME}/config/
   fmwconfig/ovd/default/keystores/adapters.jks
   -Djavax.net.ssl.trustAnchors=${DOMAIN_HOME}/config/fmwconfig/ovd/default/
   keystores/adapters.jks"
   export API_CAINFO=${DOMAIN_HOME}/config/fmwconfig/essconfig/essbase/
   walletssl/certwallet.pem
   ```

For Windows: similarly edit `%ORACLE_HOME%\bin\setWlstEnv.cmd`

```
export WLST_PROPERTIES="-Dweblogic.ssl.JSSEEnabled=true
-Dweblogic.security.SSL.enableJSSE=true
-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.CustomTrustKeyStoreType=JKS
-Dweblogic.security.TrustKeyStore=CustomTrust
-Dweblogic.security.CustomTrustKeyStoreFileName=%DOMAIN_HOME%
\config\fmwconfig\ovd\default\keystores\adapters.jks
-Djavax.net.ssl.trustAnchors=%DOMAIN_HOME%
\config\fmwconfig\ovd\default\keystores\adapters.jks"
export API_CAINFO=%DOMAIN_HOME%
\config\fmwconfig\essconfig\essbase\walletssl\certwallet.pem
```

4. Add rows of code as follows:
   For Linux: add the following lines rows of code to `${DOMAIN_HOME}/nodemanager/nodemanager.properties` (expand ${DOMAIN_HOME}).

   ```
   KeyStores=CustomIdentityAndCustomTrust
   CustomIdentityKeystoreType=jks
   CustomIdentityKeyStoreFileName=${DOMAIN_HOME}/security/keystore.jks
   CustomIdentityKeyStorePassPhrase=Password1
   CustomIdentityPrivateKeyPassPhrase=Password1
   CustomIdentityAlias=ssl
   CustomTrustKeystoreType=jks
   CustomTrustKeyStoreFileName=${DOMAIN_HOME}/config/fmwconfig/ovd/default/
   keystores/adapters.jks
   CustomTrustKeyStorePassPhrase=Password1
   ```

   For Windows: add the following lines of code to `%DOMAIN_HOME%\nodemanager\nodemanager.properties` (expand %DOMAIN_HOME%).

   ```
   KeyStores=CustomIdentityAndCustomTrust
   CustomIdentityKeystoreType=jks
   CustomIdentityKeyStoreFileName=%DOMAIN_HOME%\security\keystore.jks
   CustomIdentityKeyStorePassPhrase=Password1
   CustomIdentityPrivateKeyPassPhrase=Password1
   CustomIdentityAlias=ssl
   CustomTrustKeystoreType=jks
   CustomTrustKeyStoreFileName=%DOMAIN_HOME%
   \config\fmwconfig\ovd\default\keystores\adapters.jks
   CustomTrustKeyStorePassPhrase=Password1
   ```

5. Update as follows:
   For Linux: update `${DOMAIN_HOME}/config/fmwconfig/essconfig/essbase/essbase.cfg` with the values below:

   For Windows: update `%DOMAIN_HOME%\config\fmwconfig\essconfig\essbase\essbase.cfg` with the values below:

   ```
   AgentSecurePort 6423

   EnableSecureMode true
   ```

```
EnableClearMode false
ClientPreferredMode SECURE
```

6. Update credentials and OPSS key stores.
For Linux: Replace ${DOMAIN_HOME} in .wlst script to the actual path.

```
source ${DOMAIN_HOME}/bin/setWlstEnv.sh

${ORACLE_HOME}/oracle_common/common/bin/wlst.sh <<EOF
wlAddress='t3s://<fqdn>:<AdminServer SSL port>'
wlUser='<user name>'
wlPassword='<password>'
keystorePath='${DOMAIN_HOME}/config/fmwconfig/essconfig/essbase/walletssl/
keystore.jks'
connect(wlUser, wlPassword, wlAddress)
svc = getOpssService(name='KeyStoreService')
svc.importKeyStore(appStripe='essbase', name='internalidentity',
password='Password1', aliases='orakey', keypasswords='Password1',
type='JKS', permission=true, filepath=keystorePath)
svc.importKeyStore(appStripe='essbase', name='internaltrust',
password='Password1', aliases='orakey', keypasswords='Password1',
type='JKS', permission=true, filepath=keystorePath)
updateCred(map='oracle.essbase', key='ssl.passphrase',
user='ssl.passphrase', password='Password1') exit()EOF
```

For Windows: Replace %DOMAIN_HOME% in .wlst script to the actual path.

```
call %DOMAIN_HOME%\bin\setWlstEnv.cmd
call %DOMAIN_HOME%\oracle_common\common\bin\wlst.cmd
```

The above command will enter you into WLST mode. Then run the following:

```
wls:\offline>wlAddress='t3s:\\<fqdn>:<AdminServer SSL port>'
wls:\offline>wlUser='<user name>'wls:\offline>wlPassword='<password>'
wls:\offline>keystorePath='%DOMAIN_HOME%\\config\\fmwconfig\\essconfig\
\essbase\\walletssl\\keystore.jks'
wls:\offline>connect(wlUser, wlPassword, wlAddress)wls:\offline>svc =
getOpssService(name='KeyStoreService')
wls:\offline>svc.importKeyStore(appStripe='essbase',
name='internalidentity', password='Password1', aliases='orakey',
keypasswords='Password1', type='JKS', permission=true,
filepath=keystorePath)
wls:\offline>svc.importKeyStore(appStripe='essbase', name='internaltrust',
password='Password1', aliases='orakey',
keypasswords='Password1', type='JKS', permission=true,
filepath=keystorePath)
wls:\offline>updateCred(map='oracle.essbase', key='ssl.passphrase',
user='ssl.passphrase', password='Password1')
wls:\offline>exit()
```

# Update TLS Certificates

You can update Transport Layer Security (TLS) self-signed certificates, when, for example, they are expired, or when you need to use several hosts for different WebLogic servers. After running the update tool, all external certificates that were added before, remain in the trust store file.

The TLS certificate update tool can be used to add or update all certificates for Essbase 21c configurations.

**Prerequisites**

1. Configure Essbase with TLS connection. See Set up Weblogic TLS Connection for Essbase.
2. Stop WebLogic.
3. Set environment variables:
   - JAVA_HOME and PATH
   - ORACLE_HOME - Path to Fusion Middleware and Essbase folder
   - DOMAIN_HOME

   See Environment Locations in the Essbase Platform.

**Update tool usage and properties file parameters**

Before updating certificates, the update tool backs up all necessary files. The update tool prompts you for the private key password.

The command to run the tool is:

For Linux:

```
java -jar ${ORACLE_HOME}/essbase/lib/tlsTools.jar <properties file>
```

For Windows:

```
java -jar %ORACLE_HOME%\essbase\lib\tlsTools.jar <properties file>
```

where:

properties file is `tls_tools.properties`, and located at the following path:

- for Linux: `${ORACLE_HOME}/essbase/bin/tls_tools.properties`
- for Windows: `%ORACLE_HOME%\essbase\bin\tls_tools.properties`

and includes the following parameter, to add external certificates to Essbase:

```
SAN=
```

`SAN` (Subject Alternative Name) parameter, which has no value by default, lets you specify the IP addresses and domain names that must be secured by the certificate update. Provide a value to the SAN parameter to indicate how Essbase should update the certificates. If the SAN

parameter has a value, all external, self-signed certificates are added. If all parameters are empty of values, all existing certificates in the Essbase environment are updated.

The format is shown below. A; all names must be separated by commas.

```
SAN="DNS:<hostname>,IP:<ip address>"
```

For example:

```
SAN=IP:10.x.x.11,IP:10.x.x.13,IP:10.x.x.17,DNS:myhost,DNS:myhost.example.com
```

**Run Java command with update tool to update certificates**

1. Add SAN parameter to `tls_tools.properties` file, as described above.
2. Run Java command as shown above.

# Add External Certificates to Essbase

You can add new external certificates to Essbase. After running the update tool, all external certificates that were added before, remain in the trust store file.

**Prerequisites**

1. Configure Essbase with TLS connection. See Set up Weblogic TLS Connection for Essbase.
2. Stop WebLogic.
3. Set environment variables:
   - JAVA_HOME
   - ORACLE_HOME - Path to Fusion Middleware and Essbase folder
   - DOMAIN_HOME

   See Environment Locations in the Essbase Platform.

**Update tool usage and properties file parameters**

Before updating certificates, the update tool backs up all necessary files.

The command to run the tool is:

For Linux:

```
java -jar ${ORACLE_HOME}/essbase/lib/tlsTools.jar <properties file>
```

For Windows:

```
java -jar %ORACLE_HOME%\essbase\lib\tlsTools.jar <properties file>
```

where

properties file is `tls_tools.properties`, and located at the following path:

- for Linux: `${ORACLE_HOME}/essbase/bin/tls_tools.properties`

- for Windows: `%ORACLE_HOME%\essbase\bin\tls_tools.properties`

and includes the following parameter, to add external certificates to Essbase:

```
certFile=
```

`certFile` parameter is the full path to additional external certificates, in PEM format. This parameter is used for adding new certificates to corresponding files, not for updating certificates.

If certFile parameter (path) has a value, certificates are added to the trust store. Any other parameters are ignored.

> **Note:**
>
> External certificates, in PEM format, are obtained using keytool or openssl.

**Run Java command with update tool to update certificates**

1. Add `certFile` parameter to `tls_tools.properties` file, as described above.
2. Run Java command as shown above.

# Add External Certificates for External Java Process

Here you see how to add external certificates for an external Java process.

**Steps for Using Partitions with Self-Signed Certificates:**

1. Navigate to relevant location below and edit the `essbase.cfg` file.
   - For Linux platform:

     ```
     ${DOMAIN_HOME}/config/fmwconfig/essconfig/essbase
     ```

   - For Windows:

     ```
     %DOMAIN_HOME%\config\fmwconfig\essconfig\essbase
     ```

2. Add the following variable to the bottom of the file and save it.

   ```
   env:API_DISABLE_PEER_VERIFICATION 1
   ```

**Steps for Using Java-based Clients with Self-Signed Certificates**

1. Run the following command if the Essbase server is configured by enabling TLS option.
   - For Linux platform:

     ```
     ${JAVA_HOME}/bin/keytool -printcert -rfc -sslserver
     <external_host>:<external_port>
     ```

- For Windows:

```
%JAVA_HOME%\bin\keytool -printcert -rfc -sslserver
<external_host>:<external_port>
```

2. The above command generates certificates. Copy the certificates into a text file.
3. Run the command below to import the certificate to java cacerts.
   - For Linux platform:

```
${JAVA_HOME}/bin/keytool -importcert -alias <hostname> -file
<certificate_file> -noprompt -trustcacerts -keystore ${JAVA_HOME}/lib/
security/cacerts -storepass Password1
```

   - For Windows:

```
%JAVA_HOME%\bin\keytool -importcert -alias <hostname> -file C:
\21.3_EsbInstaller\sca00jqv.txt -noprompt -trustcacerts -keystore
%JAVA_HOME%\lib\security\cacerts -storepass Password1
```

   Certificate is added to keystore.

**Steps for Configuring WebLogic for Use with Self-Signed Certificates**

**Caution:**

The Essbase platform includes scripts in `<DOMAIN HOME>/bin` that can customize the environment and behaviors of Essbase functionality. However, making changes to these domain environment or startup scripts can have unintended effects, including startup failure. Oracle recommends making changes in a test environment first. Before editing these scripts, always:

1. Stop the Essbase managed servers, using `<DOMAIN HOME>/esstools/bin/stop.sh` (on Linux), or `<DOMAIN HOME>\esstools\bin\stop.cmd`(on Windows).
2. In `<DOMAIN HOME>/bin`, make a backup copy of the file you want to edit. For example,

   On Linux

```
cp setStartupEnv.sh setStartupEnv_bak.sh
```

   On Windows

```
copy setStartupEnv.cmd setStartupEnv_bak.cmd
```

3. Edit carefully, using only Oracle's documented instructions, or working with Oracle Support.
4. Restart Essbase, using `<DOMAIN HOME>/esstools/bin/start.sh` (on Linux), or `<DOMAIN HOME>\esstools\bin\start.cmd`(on Windows). Check that startup completed normally.

1. Edit the relevant file:
   - For Linux platform:

     ```
     ${DOMAIN_HOME}/bin/setDomainEnv.sh
     ```

   - For Windows:

     ```
     %DOMAIN_HOME%\bin\setDomainEnv.cmd
     ```

2. Replace the following line:

   ```
   JAVA_OPTIONS="${JAVA_OPTIONS}"
   ```

   with the following string:

   ```
   JAVA_OPTIONS="${JAVA_OPTIONS} -
   Dweblogic.security.SSL.ignoreHostnameVerification=true"
   ```

3. Save the file.
4. Stop and restart the Essbase stack instance.

# Replace Self-Signed Certificates with CA Certificates

You can replace self-signed certificates with certificates sent by Certificate Authority (CA) company. After running the update tool, all external certificates that were added before, remain in the trust store file.

### Prerequisites and Notes

1. Configure Essbase with TLS connection. See Set up Weblogic TLS Connection for Essbase.
2. Stop WebLogic.
3. Set environment variables:
   - JAVA_HOME
   - ORACLE_HOME - Path to Fusion Middleware and Essbase folder
   - DOMAIN_HOME

   See Environment Locations in the Essbase Platform.
4. Validate content of Certificate Authority (CA) files:
   a. All CA-based certificate files, received from the Certificate Authority, are in PEM format (RFC 7468).
   b. One file must contain the private key; it is recommended to store it as RSA private key (RFC 3447), which supports two steps of security.
   c. All certificates in all files must form a full certificate chain, from root to user certificates.

### Update tool usage and properties file parameters

Before updating certificates, the update tool backs up all necessary files. The update tool prompts you for the private key password and replaces identity and trust store with CA-based certificates.

The command to run the tool is:

For Linux:

```
java -jar ${ORACLE_HOME}/essbase/lib/tlsTools.jar <properties file>
```

For Windows:

```
java -jar %ORACLE_HOME%\essbase\lib\tlsTools.jar <properties file>
```

where

properties file is `tls_tools.properties`, and located at the following path:

- for Linux: `${ORACLE_HOME}/essbase/bin/tls_tools.properties`
- for Windows: `%ORACLE_HOME%\essbase\bin\tls_tools.properties`

and includes the following parameter for adding CA-based certificates:

```
certCA=
```

Files in the `certCA` property are separated by a colon (:) in Linux, or a semicolon (;) in Windows.

If certCA parameter has a value, CA-based certificates are added; All other parameters are ignored)

**Run Java command with update tool to update certificates**

1. Add `certCA` parameter to `tls_tools.properties` file, as described above.
2. Run Java command as shown above.

7

# Migrate Essbase Applications

If you have existing applications from an Essbase 11g On-Premise installation, or a cloud service instance, you can migrate them.

**Topics:**



## About Migration Tools and Use Cases

Here is an explanation of various tools and uses cases for migrating Essbase applications to Essbase 21c.

### Migration Tools

The following migration tools are available on the Essbase web interface Console.

> **Note:**
>
> In relation to migration, references to *19c* in this document applies specifically to migration from Essbase 19c on OCI Marketplace deployments. Otherwise, all migration content in this document applies to migration from Essbase 21c or higher independent deployments.

- **11g Excel Export Utility**: Exports Essbase 11g On-Premise applications to application workbooks. You can use the application workbooks to re-create the applications on the current Essbase version.
- **11g LCM Export Utility**: Exports artifacts from Essbase 11g On-Premise as a `.zip` file, which you can import in to Essbase 12c or higher. This Life Cycle Management (LCM) utility can also be used to export from, and import to, Essbase 11g On-Premise. This utility packages into a zip everything you need to support migration to the current version. Download `EssbaseLCMUtility.zip`, and see the enclosed README for usage details. With the 11g LCM Export Utility, you can create applications by exporting applications and cubes. You then import them using the Essbase Command Line Interface.
- **Command Line Interface (CLI)**: A scripting interface that uses REST APIs to perform most common Essbase administrative actions. CLI includes an LCM import command you can use for migrating 11g LCM Export Utility `.zip` files exported from Essbase 11g On-Premise. The LCM export and LCM import commands also facilitate migrating applications from instances on versions 12c or higher. Use cases include:
  - Migration of applications from different instances of the same version (e.g. Dev > Test > Prod)

- Upgrade utility for migration to higher versions of Essbase

Both LCM commands are based on the REST API. You can access these commands in Essbase and run them from the following:

- Jobs in the Essbase web interface: **Export LCM** and **Import LCM** jobs. These are used for 21c to 21c migration.
- Command Line Interface (CLI): using lcmexport and lcmimport commands. lcmimport can be used to import data zip file originating from Essbase 11g, or from 19c or higher. lcmexport can be used for Essbase 21c to 21c migration. Using its login command, authenticate Essbase.
- REST API: Execute Job operation (using jobtypes lcmExport and lcmImport)

> **Note:**
>
> LCM export command can be used to export an application to a zip file and then LCM import is used to import it to the target version of Essbase. LCM Import command can alternatively be used to migrate an application originating from Essbase 11g On-Premise (exported from 11g using the 11g LCM Export Utility to an export zip file and then imported from the zip file it to the target Essbase command-line).

- **Migration Utility**: Manage migration of an entire Essbase instance, for Essbase 12c or higher. In addition to migrating application artifacts, this utility also helps you migrate user role assignments and users/groups from supported identity providers. Download `migrationTools.zip`, and see the enclosed README for usage details. The tool supports migration from Essbase 19c or Essbase 21c. Use the Migration Utility between major versions and between un-patchable releases to ensure database schema integrity after migration. Not supported for use with EPM Shared Services security mode.

# Migrate From Essbase 11g On-Premise

You can migrate Essbase 11g On-Premise applications, cubes (databases), and users.

Moving all elements to the same data center, particularly for large volumes of data, removes uncertainty about added network latency. Files and databases are local to Essbase and are accessed as efficiently as if they were based on-premises. You can use the 11g LCM Export Utility, to export an on-premises cube to a zip file, and then use the Command Line Interface (CLI) to import the zip file that imports Essbase 11g On-Premise applications, folders, and elements.

**Topics:**



## Prepare to Migrate from Essbase 11g On-Premise

If you have an existing Essbase 11g On-Premise application and cube to migrate to Essbase 21c, review the following considerations and prerequisites.

**Differences Between Essbase 11g On-Premise and Essbase 21c**

- Free-form data exports and imports for cubes with typed measures behaves differently in Essbase 21c. For the latest information, see Loading, Clearing, and Exporting Text and Date Measures.
- Before you migrate, review the Differences Between Essbase 11g and Oracle Essbase 21c.

**Task Flow for Migrating**

> **Note:**
>
> - If you used EPM Shared Services in Essbase 11g On-Premise to configure an external security provider, then step 1 below isn't required. Based on the security mode chosen during configuration, you may need to configure your target EPM instance or WebLogic to use the same external security provider as used in Essbase 11g On-Premise.
> - If you're using Oracle Identity Cloud Service, configure it to use the same external security provider as used in Essbase 11g On-Premise.

1. Migrate users and groups from source Essbase 11g On-Premise EPM Shared Services to OCI Identity and Access Management (IAM) or Oracle Identity Cloud Service (IDCS) (for OCI deployment) or EPM Shared Services / WebLogic LDAP (for Independent deployments). See Migrate Essbase 11g Users and Groups.
2. If you're exporting non-Unicode Essbase 11g On-Premise applications, you must convert the applications to Unicode.
   a. Use Alter System on the server, and then on a backup copy of the Essbase application, prior to running 11g LCM Export Utility, to enable Essbase itself to support the Unicode application.
   b. For non-Unicode, **block** storage applications, export the application using `-converttoutf8` option in the export command. See 11g LCM Export Utility Options.

      For non-Unicode, **aggregate** storage applications, follow the manual Unicode conversion instructions in Convert Non-Unicode Aggregate Storage Application to Unicode Mode.
3. Migrate 11g applications:
   a. Export Essbase applications using the 11g LCM Export Utility, downloaded from target Essbase 21c instance, and running the utility on the computer where Essbase 11g On-Premise is installed.

      > **Note:**
      >
      > To use the 11g LCM Export Utility, Java Development Kit (JDK) 8 or higher must be installed, and the following variables must be set: JAVA_HOME environment variable, and EPM_ORACLE_HOME and EPM_ORACLE_INSTANCE variables in the shell terminal.

   b. Import Essbase applications using the Essbase Command Line Interface (CLI) Utility, downloaded from the Essbase 21c instance. Run the utility for each exported zip file.

**Supported Essbase Versions and Paths**

The following releases have been tested for migration: 11.1.2.3.0*nn*, 11.1.2.4.0*nn*, 12.2.1, and later.

> **Note:**
>
> Migration from 11.1.2.3 is supported, however, not every application can be migrated from 11.1.2.3 to 21c. We recommend that you upgrade from 11.1.2.3.0.n.n to 11.1.2.4.0.n.n before attempting the migration to 21c.

The following migration paths are not supported:

- Essbase 19c or 21c on OCI (Marketplace deployment) to Essbase 21c on Windows (independent deployment)
- Essbase 21c on Linux (independent deployment) to Essbase 21c on Windows (independent deployment)

**Migrated 11g Artifacts**

Review the 11g artifacts that are supported for migration. See Migrated 21c Artifacts.

**Unsupported Application and Database Settings**

The following application- or database-level settings aren't supported in migration: disk volumes.

**CONFIGURATION NOTES**

- **Hybrid Mode**

  The default calculation and query processor is hybrid mode. Hybrid mode enables block storage cubes to have dynamic, upper-level sparse members, and fully dynamic query and calculation. You can query data immediately after updating it, without running batch calculations. In hybrid mode, there is no impact to your cubes if you choose not to apply dynamic calc to upper-level sparse members. Note: Hybrid mode is not the default if using calculation scripts - if your calculation scripts contain many sparse dependencies, consider enabling hybrid mode for calculation scripts as well.

- **Implied Sharing**

  If you use the IMPLIED_SHARE configuration setting in your Essbase 11g On-Premise application, your implied sharing setting is migrated, for minimal disruption. For more details about implied sharing defaults in Essbase 21c, see the IMPLIED_SHARE_ON_CREATE configuration topic.

- **Warning Regarding the UPPERCASECONNECTION esssql.cfg Setting**
  If your environment has an `esssql.cfg` file containing the no longer supported UPPERCASECONNECTION setting, you may get a warning like the following while performing data load operations:

  ```
  WARNING - 1021037 - SQL Config file syntax error [UpperCaseConnection], ignored.
  ```

  The way to fix this is to manually remove the UPPERCASECONNECTION setting from `esssql.cfg`, which is located in

  ```
  <DOMAIN_HOME>/config/fmwconfig/essconfig/essbase/esssql.cfg
  ```

  and then restart the Essbase servers.

- **Text and Date Measures**
  Starting with Essbase 21.3 and higher, the configuration ALLOWOUTOFRANGELOAD is deprecated and the behavior will be the same as "ALLOWOUTOFRANGELOAD TRUE" in previous versions. Out of range and missing values of typed measures will be loaded to, and exported from, cubes that have textual measures. In the following data export file example, the `<OutOfRange_Name>` is" Invalid" and "NoColor" for Missing values.

  ```
  "Color1" "Color2"
  "Shoes" "Massachusetts" "Q1" "#Txt:NoColor" "#Txt:Yellow"
  "Q2" "#Txt:Green"
  "Connecticut" "Q1" "#Txt:Green" "#Txt:Invalid"
  ```

  For information on loading out of range values, refer to Loading, Clearing, and Exporting Text and Date Measures.

- **Configuration Settings**

  Some default configuration values are different than they were in Essbase 11g On-Premise. Check the Configuration Reference.

  INDEXCACHESIZE and DATACACHESIZE settings now control cache sizes for all Essbase cubes (except for aggregate storage cubes). Formerly, these settings only affected newly created or migrated cubes.

  To modify the default values for application-level configuration settings, you use the Essbase web interface, as described in Set Application-Level Configuration Properties.

  Oracle recommends managing most configurations at the application level. When you migrate applications, your application-level configuration is preserved during the LCM export and import processes. Some configurations, however, are only applicable to the Essbase Server. Most of these server configurations you specify while configuring Essbase during deployment, but you can also change server configuration defaults using essbase.cfg, if needed.

**GENERAL NOTES**

- **Imported SQL Timestamp Data Types**

  SQL timestamp data types that formerly displayed in ODBC format `[yyyy-mm-dd hh:mm:ss]` now display in a different format `[dd-MON-yy hh.mm.ss.mmm a]`, in the rules editor of the Essbase web interface and everywhere else that timestamp data types are imported. To load timestamp in the format of your choosing during data loads or dimension builds, you can convert timestamps to your chosen string format by using a SQL conversion function in the query section of the load rule. The following SQL query example uses the format function: `SELECT introdate, format(introdate, 'yyyy-MM-dd hh:mm:ss') FROM tbc.dbo.product`

- **Upgrading EPM Applications - Calculations and Filters**

  After upgrading applications to Essbase 21c, you can't provision members to calculations or filters from EPM Shared Services console. You must use the Essbase web interface to assign members. Refer to: Assigning Filters and Access to Calculations.

- **Partitions**

  When you perform the LCM import operation, import the source applications before the target applications. If you don't import source applications prior to target applications, then the partition definition won't work, and you must re-create the partition definition after importing source applications.

After you roll back an OPatch, you may need to recreate transparent and replicated partitions, and re-validate the partitions.

- **Application Creation Options Other than LCM**

  In addition to using LCM to migrate exported applications, you can also create applications in the following ways:

  – Import using Excel application workbooks

  – In Smart View, use the Cube Designer extension

  – MaxL create application statement

- **Location Aliases**

  LCM doesn't support Location alias credentials migration. After you migrate your applications from Essbase 11g On-Premise, you must replace your location aliases. You can use the following automated method, or a manual method using MaxL.

  **Automated method to replace location aliases**

  1. Unzip the LCM exported zip.
  2. Go to {ApplicationName}\Databases{dbName}\Location Aliases.
  3. Open the file under this directory. This is an XML format file, where userName and password field are empty. You can provide the credentials.
  4. Zip the directory again.
  5. Import the application using the zip directory.
     *Sample xml file*

```
<?xml version="1.0" encoding="UTF-8"?>
<java version="$VERSION$" class="java.beans.XMLDecoder">
<object class="oracle.essbase.lcm.essbase.EssbaseLocationAlias">
<void property="aliasAppName">
<string>
{appName}
</string>
</void>
<void property="aliasCubeName">
<string>
{dbName}
</string>
</void>
<void property="aliasHostName">
<string>localhost</string>
</void>
<void property="password">
<string>password</string>
</void>
<void property="userName">
<string>lauser</string>
</void>
</object>
</java>
```

  **Manual method using MaxL to replace location aliases**

  An alternative option manual method uses MaxL. After you import source applications by performing the CLI LCMImport job, re-create location aliases using Create Location Alias.

- **Custom-Defined Functions and Macros**

  FOR INDEPENDENT DEPLOYMENTS - If you have custom .jar file that you use for custom-defined calculation functions and macros, these are not migrated by the 11g LCM Export Utility. You must move them manually. To do this,

  1. Note the location of your `<Essbase Path>` and `<Application directory>` (*ARBORPATH*) in Essbase 21c. Refer to Environment Locations in the Essbase Platform if needed.
  2. Migrate global (system-level) functions by copying your `.jar` files from `<Essbase Path>/java/udf` on your source instance to `<Essbase Path>/java/udf` on your target Essbase instance.
  3. Migrate local (application-level) functions by copying your `.jar` files from the application directory on your source instance to the application directory on your target Essbase instance. In other words, copy the `.jar` files from `<ARBORPATH>/app/<app_name>` on your 11g server to `<Application directory>/app/<app_name>` on your 21c server.
  4. On your target Essbase instance, add JVMMODULELOCATION to `essbase.cfg`, providing as an argument the path to the JVM library on your system.

- **Client Service URLs**

  FOR INDEPENDENT DEPLOYMENTS - In Essbase 11g, Provider Services is the middle-tier data-source provider to Oracle Essbase for Java API, Smart View, and XML for Analysis (XMLA) clients.

  Provider Services functionality is integrated with WebLogic. Update the client URLs to the current format.

| Clients | Former URL for Connecting Provider Services to the Specified Client | New URL in Essbase 21c |
|---|---|---|
| Java API | `http://server_name:port/aps/JAPI` | `http://server_name:port/essbase/japi` |
| Smart View | `http://server_name:port/aps/SmartView` | `http://server_name:port/essbase/smartview` |
| XML for Analysis (XMLA) | `http://server_name:port/aps/XMLA` | `http://server_name:port/essbase/xmla` |

- **Outline Solve Order and Enabled Typed Measures**

  FOR OCI MARKETPLACE DEPLOYMENTS - After you migrate an Essbase application from Essbase 11g On Premises server to Essbase deployed on OCI via Marketplace, you must enable typed measures in the outline before you can change the outline solve order.

  In Essbase deployed on OCI, the **Typed Measures Enabled** outline property is set to FALSE by default. In order to change the solve order, the Typed Measures Enabled property first needs to be changed to TRUE. To change this property, see About Typed Measures in *Database Administrator's Guide for Oracle Essbase*.

## Migrated Essbase 11g Artifacts

The following table describes which global, application-level, and cube-level Essbase artifacts you can migrate from Essbase 11g On-Premise, using the 11g LCM Export Utility. A `.zip` file, created by the 11g LCM Export Utility, contains the artifacts of the exported application.

> **Note:**
>
> After upgrading EPM applications to Essbase 21c, you can't provision members to calculations or filters from EPM Shared Services console. You must use the Essbase web interface to assign members. See topics: Assigning Filters and Access to Calculations.

| Artifact | Supported for migration | Exceptions/Comments |
|---|---|---|
| Application and cube metadata | yes | Application metadata includes application type and settings. Cube metadata includes cube properties and settings. |
| Calculation scripts | yes | Application- and cube-level calculations are migrated. To see the calculation scripts, you must move application-level scripts to the cube level using the file catalog. If users and groups are already migrated before importing the application, then User/Group - Calc associations would also be imported. |
| Custom-defined functions and custom-defined macros | no | Any jar files used by Custom-defined functions must be manually migrated. |
| Data | yes | To be migrated, data must be in the cube directory in the file catalog. |
| Disk volumes | no | Disk volume definitions are not applicable. |
| Drill through definitions | yes | - |
| Excel workbooks and files | yes | - |
| Filters | yes | Cube-level filters and user-created filters are migrated. If users and groups are already migrated before importing the application, then User/Group - filter associations would also be imported. |
| Linked Reporting Objects (LROs) | no | - |
| Location aliases | no | Location aliases are migrated with the cube. LCM doesn't support location alias credentials migration. After you migrate your applications from Essbase 11g On-Premise, you must replace your location aliases. See Location Aliases section in Prepare to Migrate from Essbase 11g On-Premise. |
| Log files | no | - |

| Artifact | Supported for migration | Exceptions/Comments |
|---|---|---|
| MDX Reports | no | MDX scripts, triggers, and macros are not supported **for migration from** 11g Essbase, and therefore are NOT migrated, and not upgraded to Essbase 21c in EPM. |
| Outlines and formulas | yes | - |
| Partitions | yes | Replicated and transparent partitions are migrated.<br>Only partition definitions from the target cube are exported to the file system.<br>When migrating the partitioned cubes, you must import the source cube before the target cube; otherwise, partition definitions may not be restored. |
| Report scripts | yes | Report scripts are migrated at both application and cube levels. |
| Rule files, text files, .csv files | yes | Application- and cube-level files are migrated. |
| Scenarios | no | LCM export operations and Migration Utility export do not support migration of scenarios for applications. |
| Substitution variables | yes | Application- and cube-level substitution variables are migrated. Server-level substitution variables are migrated if you use the optional `-include-server-level` option. |
| Users | no | - |
| User roles | - | User roles are migrated if you use the `-exportepmroles` option. |

## Convert Non-Unicode Aggregate Storage Application to Unicode Mode

Before exporting an aggregate storage application from Essbase 11g On-Premise in preparation for migration to Essbase 21c, convert it to unicode mode.

> **Note:**
>
> Other references for ESSCMDQ workaround information are: How to Use ESSCMDQ to Compact Outlines (Doc ID 1534496.1) and Essbase 21c Compress Dimension Option Not Visible in JET UI (Doc ID 2853804.1).

**Client-side configuration - To set up ESSCMD/ESSCMDQ on a Windows Client**

1. From the Essbase 21c web interface, download the Essbase Client for Windows and the MaxL Client.

2. Extract the MaxL Client to a `MaxLClient` directory.
3. Extract the ESSCMD client to an `EssbaseClient` directory.
4. Copy the `startMAXL.bat` script from the `MaxLClient` directory to the `EssbaseClient` directory. Rename the script to `startEsscmd.bat`.
5. Edit the `startEsscmd.bat` file, and add a new setting to call **esscmd**, instead of **esscmd.sh**:

   ```
   "%ESSBASEPATH%\bin\esscmd" %*
   ```

6. Save the file. Run it as administrator and test logging into Essbase 21c Marketplace or Independent deployment.

   Login syntax:

   ```
   login https://<servername_or_IP>/essbase/agent <user> <password>
   ```

7. After you confirm that it works, download ESSCMDQ for Windows from https://www.oracle.com/middleware/technologies/esscmdq-sampleapps-downloads.html.
8. Extract `ESSCMDQ.exe` to the `EssbaseClient/bin` directory.
9. Copy the `startEsscmd.bat` script to `startEsscmdQ.bat`.
10. Edit the `startEsscmdQ.bat` file to call **esscmdq** instead of **esscmd**:

    ```
    "%ESSBASEPATH%\bin\esscmdq" %*
    ```

11. Save the file. Run it as administrator and test logging into Essbase 21c Marketplace or Independent deployment.

    Login syntax:

    ```
    login https://<servername_or_IP>/essbase/agent <user> <password>
    ```

> **Note:**
>
> - Do not use an IDCS/MSAD userid to connect. Use a 'native' user to login.
> - If using a proxy server, you may need to add the following settings to the startEssmcd/q.bat scripts:
>   - set HTTP_PROXY=<proxyserver>:<port>
>   - set HTTPS_PROXY=<proxyserver>:<port>

**Server-side configuration - To set up directly on the Essbase server**

1. Convert the copied aggregate storage application to Unicode mode using MaxL Shell, as described below.
2. Change the ESSLANG value within the source outline from native encoding to UTF-8, as described below.

**Convert the copied aggregate storage application to Unicode mode using MaxL Shell:**

1. Log in to the source Essbase 11g On-Premise instance using MaxL Shell.

2. Execute MaxL statement `alter application <copied_app> set type unicode_mode` to convert the application to Unicode.

   For example:

   ```
   MaxL> alter application SampleBck set type unicode_mode;
   ```

   For more details on the MaxL, see Alter Application (Aggregate Storage).

> **Note:**
>
> All of the following operations must be performed on the copied application and not the source application.

**Change the ESSLANG value within the source outline from native encoding to UTF-8.**

1. Download ESSCMDQ
   a. Download platform-specific "11.1.2.4.010+" version of ESSCMDQ from Download ESSCMDQ to your source EPM 11g instance.
   b. Unzip the files directly to the same directory where ESSCMD is present in the installation,
   **For Linux**

   `$ESSBASEPATH/bin`

   For example:

   ```
   ./Middleware/EPMSystem11R1/products/Essbase/EssbaseServer/bin/ESSCMDQ
   ```

   **For Windows**

   `%ESSBASEPATH%\bin`

   For example:

   ```
   .\Middleware\EPMSystem11R1\products\Essbase\EssbaseServer\bin\ESSCMDQ.exe
   ```

   To know the values of environment variables in your source EPM 11g installation, check the environment file.

   **For Linux**:

   ```
   ./Middleware/user_projects/<epm_instance>/EssbaseServer/
   essbaseserver1/bin/setEssbaseEnv.sh
   ```

   **For Windows:**

   ```
   ./Middleware/user_projects/<epm_instance>/EssbaseServer/
   essbaseserver1/bin/setEssbaseEnv.bat
   ```

   By default, `<epm_instance>` would be `epmsystem1`.
   c. Make a copy of the existing script

**For Linux**

```
./Middleware/user_projects/epmsystem1/EssbaseServer/essbaseserver1/bin/
startEsscmd.sh
```

as

```
./Middleware/user_projects/epmsystem1/EssbaseServer/essbaseserver1/bin/
startEsscmdQ.sh
```

**For Windows**

```
.\Middleware\user_projects\epmsystem1\EssbaseServer\essbaseserver1\bin\s
tartEsscmd.bat
```

as

```
.\Middleware\user_projects\epmsystem1\EssbaseServer\essbaseserver1\bin\s
tartEsscmdQ.bat
```

Within this newly created script, change the call from `ESSCMD` to `ESSCMDQ`.

d. Just before this last line (just before the call to ESSCMDQ), add the following lines:

**For Linux**

```
export ESSCMDQ_UTF8MODE=1
export ESSLANG=.UTF-8@Binary
```

**For Windows**

```
set ESSCMDQ_UTF8MODE=1
set ESSLANG=.UTF-8@Binary
```

2. Make sure that you have stopped the copied application before converting the outline.
3. Now create a `client` folder under ARBORPATH.
4. Copy the application folder from `ARBORPATH/app` directory to client directory. For ASOBck app, for example:

   **For Linux**

   ```
   $ARBORPATH/app/ASOBck as $ARBORPATH/client/ASOBck
   ```

   **For Windows**

   ```
   %ARBORPATH%\app\ASOBck as %ARBORPATH%\client\ASOBck
   ```

5. Execute the following commands in ESSCMDQ after launching the following.

> **Note:**
>
> ESSCMDQ is interactive, so parameters for each command can be found in interactive mode. To see what a parameter means, enter the command, such as OpenOtl, and then press Enter to see the menu explaining the parameter. Or enter the ESSCMDQ command and press Enter, without any parameters, and the parameter menu is displayed.

**Linux example**

```
./Middleware/user_projects/epmsystem1/EssbaseServer/essbaseserver1/bin/
startEsscmdQ.sh
openotlex2 1 1 appName dbName outlineName Y Y Locale N 0


writeotlex 0 1 1 appName dbName outlineName 2
```

**Windows example**

```
.\Middleware\user_projects\epmsystem1\EssbaseServer\essbaseserver1\bin\star
tEsscmdQ.bat
openotlex2 1 1 appName dbName outlineName Y Y Locale N 0


writeotlex 0 1 1 appName dbName outlineName 2
```

Note that `Locale` should be the native ESSLANG value used in the source Essbase 11g On-Premise environment.

For example (Linux syntax)

```
mkdir $ARBORPATH/client
cp -r $ARBORPATH/app/ASOBck $ARBORPATH/client

./Middleware/user_projects/epmsystem1/EssbaseServer/essbaseserver1/bin/
startEsscmdQ.sh
openotlex2 1 1 ASOBck Basic Basic Y Y "Japanese_Japan.MS932@Binary" N 0
writeotlex 0 1 1 ASOBck Basic Basic 2
exit
```

6. Make sure that no errors are displayed while executing the above commands. Then, for each cube, copy just the outline file from the client directory back to the application directory.

   For example (Linux syntax):

   ```
   #Now copy back the converted outline only for each cube. For ASOBck app -
   cp $ARBORPATH/client/ASOBck/Basic/Basic.otl $ARBORPATH/app/ASOBck/Basic/
   Basic.otl

   #Note: The artifact files (.txt or .csc), which were created in native
   ```

```
locale, may need to be converted to UTF-8 manually using third party tools
which help in converting text encoding.
```

7. Launch ESSCMDQ again using:

   **For Linux**

   ```
   ./Middleware/user_projects/epmsystem1/EssbaseServer/essbaseserver1/bin/
   startEsscmdQ.sh
   ```

   **For Windows**

   ```
   .\Middleware\user_projects\epmsystem1\EssbaseServer\essbaseserver1\bin\star
   tEsscmdQ.bat
   ```

   and restructure each cube.

   ```
   #Please replace hostname, username, password, appname and cubename with
   appropriate values
   login 'hostname' 'username' 'password'
   select appname cubename
   openotl 2 1 appname cubename outlinename y y 0
   writeotl 0 2 1 appname cubename outlinename
   restructotl 1
   closeotl 0
   unlockobj 1 appname cubename outlinename
   logout
   exit
   ```

   For example:

   ```
   login localhost:1423 user password
   select ASOBck Basic
   openotl 2 1 ASOBck Basic Basic y y 0
   writeotl 0 2 1 ASOBck Basic Basic
   restructotl 1
   closeotl 0
   unlockobj 1 ASOBck Basic Basic
   logout
   exit
   ```

# Migrate Essbase 11g Users and Groups

The task flow for migrating Essbase users and groups from Essbase 11g On-Premise to Essbase 21c varies depending on your identity provider and details about your applications.

**Prerequisites and Considerations**

- If, for your Essbase 11g On-Premise instance, you stored users and groups natively in EPM Shared Services, you need to export those users and groups, to import them into your security provider for Essbase 21c. Reformatting of the exported user and group files may be required if you're migrating from Shared Services into WebLogic Embedded LDAP.

Shared Services security is recommended only for Essbase customers who also use EPM applications and have user overlap between EPM applications and “stand-alone” Essbase applications. Essbase customers who don't use any EPM applications are recommended to migrate to Essbase using the default WebLogic security, and not Shared Services. WebLogic security can be federated with many external authentication identity providers. See WebLogic Authentication.

- If you want filters and calculation assignments of existing users to be migrated, ensure that Essbase has the same set of users and groups already available.
- If you're using native (default) identity providers, migrate users and groups from Essbase 11g On-Premise by exporting them to a CSV file and importing them after you install and configure Essbase 21c. If you're using federated/external providers, integrate these with Essbase 21c.
- When you import user names, the following special characters are not allowed in the name.

  ```
  # ; , = + * ? [ ] |< > \ " ' / [Space] [Tab]
  ```

  The name length is limited to 50 characters.

**Scenarios for Migrating users and groups**

**Scenario 1 - Exporting users/groups from Essbase 11g and importing them into Essbase 21c, which is configured in Shared Services mode**

**Exporting users/groups**

- If the native Shared Services directory is used in the source EPM instance, then export users and groups using Shared Services Console. See Migrating Native Directory (Security). You should only select users and groups, and don't migrate roles, while exporting from EPM Shared Services. User roles are migrated by the Essbase 11g LCM Export Utility.
- If a source Shared Services instance is configured to use an external security provider, then no explicit user/group export is required.

**Importing users/groups**

- If native Shared Services directory is used in the target EPM instance, then import users and groups using Shared Services Console.
- If the source EPM instance was configured to use an external security provider (including when you use MSAD or other LDAP-based user directories), then configure the target Shared Services instance with the same provider details. See Configuring OID, Active Directory, and Other LDAP-based User Directories.

**Options for the Shared Services Administrator**

If you want to import the Shared Services administrator user from an Essbase 11g On-Premise instance to an Essbase 21c instance configured to use EPM Shared Services for authentication, the following considerations can help you avoid pitfalls.

Before any user migration steps, ensure you have a dedicated EPM Foundation-only instance of Shared Services that you have configured with Essbase 21c. This Shared Services instance already has a Shared Services administrator.

> **Caution:**
>
> If the Shared Services administrator in the source 11g EPM instance isn't the same administrator that you configured in the target EPM Foundation-only instance, and you include this source administrator in the CSV file when you import users to your EPM Foundation-only Shared Services configured with Essbase 21c, your target Shared Services administrator will be overwritten by the 11g Shared Services administrator.

To handle this, select an option:

- **Only Use 11g Administrator**

  Allow the source Shared Services administrator to overwrite the target administrator.

  1. Export all users from Essbase 11g On-Premise to a CSV file, including the Shared Services administrator.
  2. Import all users to the target, empty EPM Foundation-only instance.
  3. Log in on the target instance as the 11g Shared Services administrator, and assign roles and permissions to users. Your Shared Services administrator user in the target instance retains the same user ID, but has the password you specified during configuration on the target instance.

- **Only Use Target Administrator**

  Remove the 11g Shared Services administrator from the export file, so that the target administrator will not be overwritten.

  1. Export all users from Essbase 11g On-Premise to a CSV file, including the Shared Services administrator.
  2. From the export CSV file, remove the row containing the administrator.
  3. Import the rest of the users to the target, empty EPM Foundation-only instance.
  4. Log in as the target Shared Services administrator, and assign roles and permissions to users.

- **Keep Both Administrators**

  Take steps to migrate the 11g Shared Services administrator without affecting the target administrator.

  1. Export all users from Essbase 11g On-Premise to a CSV file, including the Shared Services administrator.
  2. Edit the CSV file to remove the **internal_id** value associated with the source Shared Services administrator. This removes the Shared Services and Essbase administrator role, but keeps the user ID and password intact.
  3. Import the users to the target EPM Foundation-only instance. The Shared Services administrator's user ID is migrated, but no longer has administrator role.
  4. Log in as the target Shared Services administrator and grant whichever role you want to give to the 11g Shared Services administrator user ID you just migrated.

**Scenario 2 - Exporting users/groups from Essbase 11g and Importing them into Essbase 21c, which is configured in WebLogic security mode**

**Exporting users/groups**

- If native Shared Services directory is used in the source EPM instance, then export users and groups using Shared Services Console. See Migrating Native Directory (Security).
- If source Shared Services instance is configured to use an external security provider, then no explicit user/group export is required.

**Importing users/groups**

- If native Shared Services directory was used in the EPM 11g instance, then you may need to manually convert the file exported from Shared Services to a format that WebLogic security mode can understand.
  1. Open the users/groups zip files exported by Shared Services, and extract the files `"resource\Native Directory\Users.csv"` and `"resource\Native Directory\Groups.csv"` as target 21c files.
  2. Manually assign groups as follows: user group associations should be extracted from the source Essbase 11g CSV file, added to the target Essbase 21c CSV file, and then later imported into the Essbase 21c interface.
  3. Manually re-order the columns in these target 21c CSV files to a format that contains the user ID, first and last names (optional), email address (optional), password (optional) and role type (User, Power User, or Service Administrator).
  4. Please specify the role type field in these target CSV files as "User".
  5. Import the modified target CSV files using the Essbase 21c interface, logged in as a Service Administrator. Go to the Applications home page > Security > Import. Browse to the .csv files, and click **Import**.
- If source EPM instance was configured to use an external security provider, then please configure WebLogic with the same security provider details. See Configuring Authentication Providers.
- Your existing Essbase 11g On-Premise instances use Shared Services security, with users and groups stored natively in Shared Services or with users and groups stored in an external identity provider.

  During configuration of Essbase 21c, you chose a security mode: either embedded WebLogic or Shared Services. Regardless of the selected security mode, if your Essbase users and groups exist in an external identity provider, you should integrate Essbase 21c with that provider. See WebLogic Authentication and EPM Shared Services Authentication, and their subtopics on external identity providers.

> **Note:**
>
> Reformatting of the exported user and group files may be required if you're migrating from Shared Services into WebLogic Embedded LDAP.

> **Note:**
>
> Shared Services security is recommended only for Essbase customers who also use EPM applications and have user overlap between EPM applications and “stand-alone” Essbase applications. Essbase customers who don't use any EPM applications are recommended to migrate to Essbase using the default WebLogic security, and not Shared Services. WebLogic security can be federated with many external authentication identity providers. See WebLogic Authentication,

### User Roles for Access

Assignment of user roles behavior differs from Essbase 11g On-Premise if you choose Essbase to run in WebLogic security mode. Database Access is now the lowest role, and has, by default, read access to data values in all cells. To restrict access to data values, you must create a NONE filter and assign it to users and groups. This was not a requirement in Essbase 11g On-Premise, where Filter was the lowest role, and has, by default, no access to data values in all cells.

The following Essbase security artifacts are migrated using the 11g LCM Export Utility: Essbase server-level roles, application-level roles, filter associations, and calc associations. If you choose to migrate to an Essbase instance that uses WebLogic security, LCM handles provisioning users and groups with the corresponding new roles. Note that this mapping isn't applicable if your target Essbase instance is configured to Shared Services security and the same 11g roles would remain in Essbase.

**Table 7-1 Default role mapping**

| Source 11g EPM Shared Services Roles | Target 21c WebLogic Embedded LDAP Roles | Level |
|---|---|---|
| Administrator | Service Administrator | Server |
| Application Manager | Application Manager | Application |
| Calc | Database Update | Application |
| Create/Delete application | Power User | Server |
| Database Manager | Database Manager | Application |
| Filter | Database Access | Application |
| Read | Database Access | Application |
| Server Access | User | Server |
| Write | Database Update | Application |

Note that Filter role in Essbase 11g On-Premise doesn't allow Read access, but allows access to members restricted by the filter. Now, there's no Filter role, and the lowest role access is Database Access, which allows Read access to all members. To restrict access to selective members, use a group filter that restricts global access.

**Required access for tasks:**

- For exporting: A user with at least Application Manager role, for the application created, can export applications, folders, and artifacts.

  In addition, the following roles can use the 11g LCM Export Utility and their corresponding operations: Service Administrator role for all applications; Create or Delete Application roles for only those applications created by the user.

- For importing: A user with at least Power User role (in WebLogic security mode) or Create or Delete application roles (in EPM security mode) can create applications (during import) and manage applications can create applications (during import) and manage applications.

### Scenario 3 - Exporting users/groups from Essbase 11g On-Premise and Importing them into Essbase 21c, which is configured with IAM or IDCS as Identity Provider

See Export 11g Users and Groups to Essbase 21c Configured with IAM or IDCS.

# Migrate an Essbase 11g On-Premises Application

You can export applications from versions 11.1.2.3.0nn, 11.1.2.4.0nn, 11.1.2.4.5nn, or 12.2.1, using the 11g LCM Export Utility, and then import them to the target version using the CLI Utility. Note that you can also run LCMImport from the Essbase Jobs tab to import applications.

This is the workflow to migrate from 11g:

1. **Download the 11g LCM Export Utility**: In the Essbase web interface, click **Console**, expand **Command Line Tools**, and download the 11g LCM Export Utility (`EssbaseLCMUtility.zip`). The downloaded utility must be copied to and run on the same machine as the Essbase 11g On-Premise or 12.2.1 installation, for Enterprise Performance Management (EPM) roles to be exported.
2. **Set export parameters**: If `-exportepmroles` option is enabled, you must set the following parameters before you run the LCM export.
   - For Linux:

     ```
     export EPM_ORACLE_HOME=/scratch/Oracle/Middleware/EPMSystem11R1
     export EPM_ORACLE_INSTANCE=/scratch/Oracle/Middleware/user_projects/
     epmsystem1
     ```

   - For Windows:

     ```
     set EPM_ORACLE_HOME=C:\Oracle\Middleware\EPMSystem11R1
     set EPM_ORACLE_INSTANCE=C:\Oracle\Middleware\user_projects\epmsystem1
     ```

3. **Set up the 11g LCM Export Utility**: Before running the utility, you must set and export the environment variables EPM_ORACLE_HOME and EPM_ORACLE_INSTANCE in the shell terminal. These variables must be the same as those used in the source EPM 11g environment. For details, see About Middleware Home, EPM Oracle Home, and EPM Oracle Instance. Also, in the uncompressed downloaded file, run `EssbaseLCM.bat` (Windows) or `EssbaseLCM.sh` (Linux), based on the platform on which you want to run the utility. Also see 11g LCM Export Utility Options.
4. **Check the /tmp directory**: You may need to change the location of the `tmp` directory. If it is full, the 11g LCM Export Utility may fail.
5. **Run the export**: When you export non-Unicode block storage applications, use `-converttoutf8` option in the LCM export command. When you export non-Unicode aggregate storage applications, manually convert them using the steps in Convert Non-Unicode Aggregate Storage Application to Unicode Mode..

   **LCM export syntax**: At the command prompt, enter the following command syntax to export one or more applications to a .zip file:

   ```
   EssbaseLCM.bat|.sh export -server essbasehost:port -user username -
   password password -application
         appname -zipfile zipfilename [-nodata] [-include-server-level] [-
   converttoutf8] [-forceutf8]
         [-generateartifactlist] [-exportepmroles] [-allApp] [-exportdata]
             [-cube] [-filetype] [-partitions] [-filters]
   ```

   Specify these options:

   `-exportepmroles` : (optional) Exports Enterprise Performance Management (EPM) roles

`-include-server-level` : (optional) Includes server-level artifacts, such as server-level substitution variables or server-level roles

`-generateartifactlist` : (optional) Generates artifact list

For example:

```
EssbaseLCM.sh export -server localhost:1423 -user admin -password password
-application Sample -zipfile Sample.zip -include-server-level -
exportepmroles -generateartifactlist
```

This exports additional artifacts: user and group server-level roles, application-level roles, calculations, and filter associations.

6. **Run the import**: To import one or more applications, use the Essbase Command Line Interface Utility (CLI) to upload the `.zip` file to target application.

   The syntax for the CLI `lcmimport` command is as follows:

   ```
   lcmImport [-verbose] -zipfilename filename [-overwrite] [-targetappName
   targetApplicationName] [-artifactlist artifactList]
   ```

   See: LcmImport: Restore Cube Files.

   When partitions exist in the source between a source application or database, and a target application or database, only partitions from the target are exported to the file system. When partitions exist between cubes being migrated, you must import the data source before the data target. Otherwise, partition definitions may not be restored.

   Roles are set only if the users are available in Oracle Identity Cloud Service. You can override default role mapping by changing the mapping in `CSSMappings.xml` provided with 11g LCM Export Utility.

7. Federated partitions are not migrated, so when moving your application and cube to another server or version, you need to delete the federated partition and recreate it in the new environment. See Federated Cube Maintenance and Troubleshooting.

8. **Upgrade aggregate storage outline version**: After import of aggregate storage applications, the outline must be upgraded using ESSCMDQ. See Upgrade Aggregate Storage Outline Version.

9. **Validate**: Log in to the Essbase web interface to see the application and cube on the Applications page.

## 11g LCM Export Utility Options

You have the following options to use 11g LCM Export Utility to export from Essbase 11g On-Premise.

**Syntax**

```
EssbaseLCM.bat|.sh export -server essbasehost:port -user username -password
password -application
      appname -zipfile zipfilename [-nodata] [-include-server-level] [-
converttoutf8] [-forceutf8]
      [-generateartifactlist] [-exportepmroles] [-allApp] [-exportdata]
          [-cube] [-filetype] [-partitions] [-filters]
```

### Notes

- You can specify `-converttoutf8` option during export to automatically convert the Essbase 11g On-Premise block storage application to Unicode, before exporting it to a `.zip` file. Note that this will convert the source block storage application to Unicode; it is recommended to run a backup before specifying this option.
- You can specify the options/arguments in any order.
- To prompt for a password, do not include the `-password` option.
- To skip the export of application data, specify `-nodata`, which is an optional argument. By default, all application data is exported.

### Command Options and Descriptions

| Option | Description |
|---|---|
| -server <essbasehost:port> | Server host name and port number. |
| -user <username> | Server user name. |
| -password <password> | Server password. Skip if you want to be prompted for the password. |
| -application <appname> | Name of application to back up. |
| -zipfile zipfilename | Optional. Name of compressed file to hold backup files. |
| -nodata | Optional. Do not include data in the backup. |
| -overwrite | Optional. Overwrite existing backup file. |
| -converttoutf8 | (Optional) Convert block storage application to Unicode. Prompts you to type `Y` to confirm. |
| -forceutf8 | (Optional) Same as `-converttoutf8`, but without any prompt. Can be used in automation scripts. |
| -exportepmroles | (Optional) Exports Essbase roles from Enterprise Performance Management (EPM) source. |
| -generateartifactlist | Optional. Generate a text file containing a complete list of the exported artifacts. You can use this text file to manage the import of artifacts. For example, you can rearrange the order of artifacts in the list to control the order in which they are imported. You can skip importing some artifacts by removing or commenting out items in the list. |
| -include-server-level | (Optional) Include server-level artifacts, such as server-level substitution variables and server-level roles. Requires system administrator role. |
| -allApp | Optional (and case-sensitive). If used instead of -application, exports all applications to a single zip file. lcmimport can accept single-application zip files or multiple-application zip files. |
| -exportdata | Optional. Only export data. |
| -cube | Optional. Export a single cube. This option can be specified along with the options to export only: data, files of certain types, partitions, or filters. |

| Option | Description |
|---|---|
| -filetype | Optional. Only export files of the specified type. Supported file types include OTL (outline), TXT (text), RUL (rule), CSC (calc script), DTR (drill through report definition), and Excel (only .xls files are exported. No .xlsx files are exported). |
| -partitions | Optional. Only export partition definitions.<br>Lifecycle Management (LCM) import operations (and Migration Utility import) are not supported for migration of federated partitions. Federated partitions must be recreated manually on the target. |
| -filters | Optional. Only export security filters. |

# Migrate From OCI Marketplace Deployment Instances

You can migrate applications and cubes (databases) from OCI Marketplace deployments, and between 19c and higher deployment instances. Learn how to prepare for migration, and review some use cases for migrating.

You can use the Essbase Command Line Interface (CLI) Utility to migrate your source application and artifacts.

You can use the Migration Utility tool to migrate multiple applications, artifacts, users, and groups at one time, from 19c and higher deployments.

- Prepare to Migrate Essbase Applications and Users
- Migrated 21c Artifacts
- Migrate Applications Using Command Line Interface
- Migrate Applications Using Migration Utility

## Prepare to Migrate Essbase Applications and Users

Here are some considerations and requirements when migrating applications to Essbase 21c, whether from independent Essbase deployments, or Essbase on OCI via Marketplace deployments.

**Considerations and requirements**

- Lifecycle Management (LCM) import and Migration Utility import do not support migration of federated partitions. Federated partitions must be recreated manually on the target, after migration from 21c to 21c.
- You can use the Essbase Command Line Interface (CLI) to migrate your source application and artifacts across deployments and releases.
- In Independent deployments, when you have a large number of applications and using LCM is not feasible to export your applications, see: Migrate Multiple Essbase Instances to a Single Shared Services Instance.
- Export and import using Migration Utility does not support migration of applications, if the Essbase instance is configured in EPM Shared Services mode; you must use CLI with LCM export and import commands.

- Restoring an application or database from a prior backup, after the application or database was re-created using LCM import, isn't supported.
- Global variables, email configuration settings, and file scanner settings must be set on the target instance before using any of the migration tools.
- Oracle Identity Cloud Service roles aren't supported in Essbase.
- Migration Utility can migrate users and groups from embedded LDAP (or from Identity Cloud Service) to Identity Cloud Service in addition to all Essbase applications.
- If you're migrating users and groups from an LDAP source to an Essbase instance, Identity Cloud Service doesn't support nested groups. Therefore, group associations to other parent groups, from an LDAP source instance, aren't migrated to Identity Cloud Service targets, when using Migration Utility.
- Any users or groups that exist with the same name in the target environment as in the source environment, aren't updated in the target.
- To run CLI or Migration Utility, use the OCI Identity and Access Management (IAM) or Oracle Identity Cloud Service (IDCS) user that you provisioned to be the initial Essbase Service Administrator during the Essbase deployment and setup.
- When you run Migration Utility for SSL connection, include the host (`-Dhttps.proxyHost`) and port (`-Dhttps.proxyPort`) proxy settings in the command line.
- Solve order applies to dynamic members in the outline and to dynamic calculation execution of dimensions and members. Adjust the solve order of dimensions and members to indicate their calculation priority. Solve order is recommended instead of using Two Pass calculation, because it's more flexible. You can set solve order for dimensions or members, or you can use the default Essbase solve order. The minimum solve order you can set is 0, and the maximum is 127. A higher solve order means the member is calculated later; for example, a member with a solve order of 1 is solved before a member with a solve order of 2. See Solve Order in Hybrid Mode.
- Free-form data exports and imports for cubes with typed measures behaves differently in 21c. For the latest information, see Loading, Clearing, and Exporting Text and Date Measures.

**Required user roles**

- For exporting: Application Manager for the application created. In addition, the following roles can use LCM commands and CLI: Service Administrator for all applications; Power User for all applications created by the Power User.
- For importing: Power User or Service Administrator, for creating new applications during import. If you use the Power User role, then the target applications are owned by the Power User used in the migration.

## Migrated 21c Artifacts

The following table describes which global, application-level, and cube-level Essbase artifacts you can migrate between cloud service instances. These artifacts migrate as described from Essbase 21c on either OCI/Marketplace or independent deployments, and from Essbase 19c on OCI/Marketplace.

| Artifact | Exceptions/Comments |
|---|---|
| Application and cube metadata | Application metadata includes application type and settings. Cube metadata includes cube properties and settings. |

| Artifact | Exceptions/Comments |
|---|---|
| Application-level configuration files | If these files exist, they're migrated. |
| Calculation scripts | Application- and cube-level calculations are migrated. |
| Catalog server | Files in the application directory are migrated. Files stored under `shared` and `users` folders aren't migrated. You can manually download them from the web interface and restore them. |
| Connections and Datasources | Using Migration Utility, system- and application-level connections and Datasources are migrated. Using CLI Utility, connections and Datasources created at the application level are migrated.<br>With both tools, you must include the following argument in `lcmexport` operations: `-include-server-level` (or its abbreviation `-isl`). |
| Data | To be migrated, data must be in the cube directory on the cloud instance. |
| Disk volumes | Disk volume definitions aren't applicable to Essbase cloud instances. |
| Drill through definitions | Drill through definitions are migrated.<br>Do not rename drill through report definitions (.dtr files). Drill through report definitions that are renamed may not be editable and may not work as expected. |
| Excel workbooks and files | Excel workbooks and files are migrated. |
| Filters | Cube-level and user-created filters are migrated. |
| Global variables | - |
| Layouts | Cube-level layouts are migrated. |
| Linked Reporting Objects (LROs) | LROs are included for backward compatibility with migrated Essbase 11g On-Premise applications. |
| Location aliases | Location aliases are migrated with the cube. LCM doesn't support Location alias credentials migration. After you migrate your applications from Essbase 11g On-Premise, you must replace your location aliases. See Location Aliases section in Prepare to Migrate from Essbase 11g On-Premise. |
| Log files | Log files aren't migrated. |
| MDX reports | Cube-level named queries are migrated. See Analyze Data with MDX Reports. |
| Outlines and formulas | Formulas containing @XREF aren't migrated. |
| Partitions | Replicated and transparent partitions are migrated.<br>Only partition definitions from the target cube are exported to the file system.<br>Lifecycle Management (LCM) import and Migration Utility import do not support migration of federated partitions. Federated partitions must be recreated manually on the target, after migration from 21c to 21c. |
| Report scripts | Application- and cube-level report scripts are migrated. The scripts are included for backward compatibility with migrated Essbase 11g On-Premise applications. |

| Artifact | Exceptions/Comments |
|---|---|
| Rule files, text files, .csv files | Application-and cube-level files are migrated. |
| Scenarios | If a cube is scenario-enabled and has a Sandbox dimension, the related scenarios are migrated. |
| Substitution variables | Application- and cube-level substitution variables are migrated. If you have global (server)-level substitution variables, you must convert them to application-level variables prior to migration, or recreate them in the Console after migration. |
| Users and groups | Users and groups are migrated using Migration Utility; they aren't migrated when using CLI tool. |
| User roles | User roles can be migrated only from one Essbase cloud instance to another. |
| Wallet files | Wallet files are migrated for the specified application. |

# Migrate Applications Using Command Line Interface

You can use Command-Line Interface (CLI) to migrate source applications and artifacts across Essbase cloud deployments and releases.

The standard migration workflow using the Command Line Interface (CLI) is as follows:

1. Download the tool and use the `lcmexport` commands to export single or multiple applications from source to a zip file.
2. Use the `lcmimport` command to import single or multiple applications from a zip file to Oracle Essbase.

When partitions exist in the source between a source application or database, and a target application or database, only partitions from the target are exported to the file system. When partitions exist between cubes being migrated, you must import the data source before the data target. Otherwise, partition definitions may not be restored.

# Migrate Applications Using Migration Utility

As an Essbase Service Administrator, you can use the Migration Utility (`migrationTools.jar`) to migrate an entire Essbase instance (all applications, users and groups, and other artifacts) from one cloud instance to another in a single process.

You can use Migration Utility to migrate from source applications and elements from Essbase deployments on OCI via Marketplace. The utility migrates multiple applications at one time. It also migrates artifacts, rules, users and groups.

Note that the Essbase Command-line Interface (CLI) commands, `lcmimport` and `lcmexport` do not migrate users and groups.

**Before** using the Migration Utility, complete the following prerequisite: Set Up the SSL Certificate.

### Use Cases for Migration Utility

Here are some use cases for migrating with the Migration Utility.

- Migrate Essbase users from WebLogic LDAP in the source to OCI Identity and Access Management (IAM) or Oracle Identity Cloud Service (IDCS) in the target.

- Use Migration Utility for basic deployments that aren't customized. If your deployment includes customizations, such as custom single sign-on solutions, use CLI instead of Migration Utility.
- When the source Essbase deployment is from
  - Essbase Marketplace on Oracle Cloud Infrastructure, using OCI Identity and Access Management (IAM) or Oracle Identity Cloud Service (IDCS), or
  - Essbase Marketplace on Oracle Cloud Infrastructure, using Embedded LDAP

  then before using the Migration utility steps below to export, first create a new confidential application as outlined in Create a Confidential Identity Application. Also, before using the Migration Utility to import, change the host and IAM or IDCS details in `import.properties` to point to the target Essbase instance.

### Steps to Migrate Cloud Applications and Users using Migration Utility

1. Before you use the Migration Utility, if you haven't already, patch your source Essbase instance to the latest version.
2. If it isn't already installed, download and install Java SE Development Kit (JDK) 8 from Oracle Technology Network.
3. Set the JAVA_HOME environment variable name on your system to point to the JDK installation folder. If the installation path contains any spaces, enclose the path in the variable value, within quotation marks, for example, `"C:\Program Files\Java\jdk1.8.0_171"`.
4. Sign in to the target Essbase web interface, and navigate to the Console.
5. In the Console, go to Desktop Tools, and expand Command Line Tools.
6. Click **Download** next to **Migration Utility**.
7. Download the Migration Utility zip file to a local drive. For best results, choose a path that has no spaces, for example, `C:\Oracle`.
8. Extract the zip file, and see the extracted files (properties, jar, and readme) in the `migrationTools` folder.
9. Before you run the Migration Utility export, edit the `export.properties` file, located in the same directory as the utility. Provide the details of the Essbase source instance that you are migrating from.

| Export Property | Description |
|---|---|
| userName | Required. Essbase administrator user name. |
| password | Required. Essbase administrator password. |
| host | Required. IP address of the load balancer, if a load balancer was configured during Essbase deployment. Otherwise, the host name or IP address that corresponds with the Essbase public IP address. |
| port | Optional. Source Essbase instance's HTTP listening port. If source instance is configured in secure (TLS) mode and `isTLS`=**true** port **443** is assumed. If source instance is configured with LDAP identity provider, set port as **80**. |
| isTLS | Optional: **true** or **false**. If true, source instance is configured in secure (TLS) mode using the specified `port` value. |
| proxy | Optional. HTTP proxy host address, if the connection to the source Essbase instance requires a proxy. Proxy host and proxy port are separated by a colon. If the proxy port is omitted, its value is assumed to be 80. Example with port omitted: `www-proxy-example.com`. Example with port included: `www-proxy-example.com:80` |

| Export Property | Description |
|---|---|
| skipdata | Optional. Default is **false**. Set to **true** if only schemas of the Essbase application should be exported. |
| skipUser | Optional: **true** or **false**. Set to true only if there is no need to export users and/or groups. Default value is false. |
| idcsHost | Required only when migrating users and/or groups from an instance deployed on OCI via Marketplace. The source's identity domain host in IAM or IDCS. From the Identity Domain URL (example: `https://idcs-<string_of_numbers_and_letters>.identity.oraclecloud.com`), extract only the domain part after the string. Example: `identity.oraclecloud.com` |
| idcsTenant | Required only for migrating users and/or groups from an instance deployed on OCI via Marketplace. The source host's identity domain tenancy identifier in IAM or IDCS. From the Identity Domain URL (example: `https://idcs-<string_of_numbers_and_letters>.identity.oraclecloud.com`), extract only `idcs-<string_of_numbers_and_letters>`. |
| clientId | Required only for migrating users and/or groups from an instance deployed on OCI via Marketplace. The source host's client identifier for OAuth authorization, found in the integrated confidential identity application. |
| clientSecret | Required only for migrating users and/or groups from an instance deployed on OCI via Marketplace. The source host's client secret for OAuth authorization, found in the integrated confidential identity application. |
| appId | Required only for migrating users and/or groups from an instance deployed on OCI via Marketplace. Identifier of the integrated confidential identity application on the OCI identity domain (IAM or IDCS). This identity application should be configured with application roles grantable to users and groups. This property enables granting roles to migrated users and groups. |

10. Edit the **`import.properties`** file, located in the same directory as the utility. Provide the details of the Essbase target instance that you are migrating to.

| Import Property | Description |
|---|---|
| userName | Required. Target instance's Essbase administrator user name. |
| password | Required. Target instance's Essbase administrator password. |
| host | Required. Target instance's IP address of the load balancer, if a load balancer was configured during Essbase deployment. Otherwise, the host name or IP address that corresponds with the Essbase public IP address. |
| port | Optional. Target Essbase instance's HTTP listening port. If target instance is configured in secure (TLS) mode and `isTLS`=**true** port **443** is assumed. If source instance is configured with LDAP identity provider, set port as **80**. |
| isTLS | Optional: **true** or **false**. If true, target instance is configured in secure (TLS) mode using the specified `port` value. |
| userPassword | Optional. Initial password to be assigned to any new users the utility migrates to the integrated identity application in IAM or IDCS. To change the passwords after migration, use the OCI Console. |
| proxy | Optional. HTTP proxy host address, if the connection to the target Essbase instance requires a proxy. Proxy host and proxy port are separated by a colon. If the proxy port is omitted, its value is assumed to be 80. Example with port omitted: `www-proxy-example.com`. Example with port included: `www-proxy-example.com:80` |
| skipUser | Optional: **true** or **false**. Set to true only if there is no need to import users and/or groups. Default value is false. |

| Import Property | Description |
|---|---|
| idcsHost | Required only for migrating users and/or groups to an instance deployed on OCI via Marketplace. Target identity domain host. From the Identity Domain URL (example: `https://idcs-<string_of_numbers_and_letters>.identity.oraclecloud.com`), extract only the domain part after the string. Example: `identity.oraclecloud.com` |
| idcsTenant | Required only for migrating users and/or groups to an instance deployed on OCI via Marketplace. The target host's identity domain tenancy identifier. From the Identity Domain URL (example: `https://idcs-<string_of_numbers_and_letters>.identity.oraclecloud.com`), extract only `idcs-<string_of_numbers_and_letters>`. |
| clientId | Required only for migrating users and/or groups to an instance deployed on OCI via Marketplace. The target host's client identifier for OAuth authorization, found in the integrated confidential identity application. |
| clientSecret | Required only for migrating users and/or groups to an instance deployed on OCI via Marketplace. The target host's client secret for OAuth authorization, found in the integrated confidential identity application. |
| appId | Required only for migrating users and/or groups to an instance deployed on OCI via Marketplace. Identifier of the integrated confidential identity application on the OCI identity domain (IAM or IDCS). This identity application should be configured with application roles grantable to users and groups. This property enables granting roles to migrated users and groups. |
| overwrite | Optional. Set to **true** if applications to be imported already exist on the target, and you want to overwrite them. Default value is false. |
| certificates | Optional. Full path to all trust certificate files for all TLS/SSL servers. For Windows, escape backslashes with another backslash. Example: `C:\\migrationTools\\all_certs.pem` |

11. Run Migration Utility in Java with the export command to export all applications, users, and groups from the Essbase source instance catalog to a compressed file.

```
java -jar -Dhttps.proxyHost=<proxy-url> -Dhttps.proxyPort=<nn>
migrationTools.jar export export.properties <new_tar_file>
```

Example:

```
java -jar -Dhttps.proxyHost=www-proxy-abcdef.example.com -
Dhttps.proxyPort=80 migrationTools.jar export export.properties
export.tar.gz
```

12. Run Migration Utility in Java with the import command to import the compressed file to the target instance.

```
java -jar -Dhttps.proxyHost=<proxy-url> -Dhttps.proxyPort=<nn>
migrationTools.jar import import.properties <existing_tar_file>
```

13. After you run the import, the data is migrated to the Essbase catalog of the target instance.

# Post-Migration and Advanced Topics

After migrating or upgrading to Essbase 21c, test that the applications are working as expected. You may need to take additional steps to import connections and artifacts. Aggregate storage outlines may require post-migration upgrade steps.

# Selective Export of Artifacts

You can control export by selectively exporting individual Essbase artifacts for cloud service migrations, using the CLI utility.

You can export individual artifacts, for example, exporting only rules, or outlines, or data, and so on. You can also use this process for periodic backup of individual artifacts.

**Selective Migration, Backup, and Export**

You can selectively export the following:

- Cube - Export just a single cube from an application.
- Essbase Files - Export particular files, such as Outline, Rule files, Drill Through reports, and others.
- Data - Export only data. This can be useful for periodic backup of data.
- Partitions - Export only partitions.
- Filters - Export only security filters of a cube.

**Supported Essbase File Types**

The following Essbase file types are currently supported for selective export.

- OTL
- TXT
- RUL
- CSC
- DTR
- EXCEL

**CLI Utility Command Options**

The following command options have been added or changed to support selective export.

| | |
|---|---|
| `-c` or `--cube <cube name>` | Exports a single cube. This option can be used by itself or combined with one of the following options. |
| `-d` or `--exportdata` | Exports data only. |
| `-ft` or `--filetype <filetype>` | Export files of the specified type. File type keywords, such as OTL or RUL, are case-sensitive and must be entered in upper case. |
| `-ep` or `--exportpartitions` | Export partitions only. |

| | |
|---|---|
| `-ef` or `--exportfilters` | Export security filters only. |

**Examples**

- Export data only, from a single cube, for example, Demo.Basic:

```
./esscs.sh lcmexport -a Demo -c Basic -z data.zip -d
```

- Export a single cube only:

```
./esscs.sh lcmexport -a Demo -z data.zip -c basic
```

- Export only text files, from all cubes under Demo:

```
./esscs.sh lcmexport -a Demo -z data.zip -ft txt
```

- Export only partitions, from all cubes under Demo:

```
./esscs.sh lcmexport -a Demo -z data.zip -ep
```

- Export only the data from all of the applications:

```
./esscs.sh lcmexport -aa -z all_data.zip -d
```

- Export only outlines, from all cubes in an instance:

```
./esscs.sh lcmexport -aa -z cubes.zip -ft OTL
```

- Export all partitions of an instance:

```
./esscs.sh lcmexport -aa -z all_partitions.zip -ep
```

- Export all security filters of a single cube:

```
./esscs.sh lcmexport -a Sample -z all_partitions.zip -c Basic -ef
```

# Selective and Ordered Import of Artifacts

You can control import of Essbase artifacts using a selection list text file, for 11g migrations (using the 11g LCM Export Utility) and for cloud service migrations (using the CLI utility).

A selection list text file contains a list of all artifacts in the exported zip that are grouped by section. You can generate the file during export using `lcmexport` command. At the end of the file is an `IMPORT` section that contains the list of artifact entries to be imported.

You can edit the file and delete, or comment, the rows of artifacts that you want to skip in the import, using `lcmimport` command. You provide the text file as an argument in `lcmimport` operation. You can also control the order of import.

**Sample selection list text file**

```
@Provisions
/Sample/Provisions/CalcAssociation.csv
```

```
@Databases/Basic/Calc_scripts
/Sample/Databases/Basic/Calc scripts/Default Calc
/Sample/Databases/Basic/Calc scripts/CalcAll.csc

# ------------IMPORT-----------------
import @Provisions
import @Databases/Basic/Calc_scripts
# ------------IMPORT----------------
```

**How to use this feature**

- When we use 11g LCM Export Utility, you can specify the optional argument `-generateartifactlist` to generate a text file containing a list of exported artifacts.
- To skip a complete category of files, such as .rul files, comment the corresponding `IMPORT` section at the end of the text file.
- To skip specific files, delete or comment those entries in the text file.
- To control the import order, rearrange the entries under any specific category into the order that you prefer them to be imported. Files are then imported in the order listed under that category. During import, specify this file using

  `-al,-artifactlist`

- Note that the `lcmimport` command has an `-overwrite` option.
  - If `-overwrite` is true, the import operation recreates the entire application. It only imports the artifacts or files that are listed in the text file.
  - If `-overwrite` is false, the import operation imports just the artifacts or files that aren't commented in the text file. It doesn't impact other artifacts already present in the target application.

**Sample use cases**

- **Import only the data from exported zip**
  You have an exported zip of Sample app and want to just import the data from Sample/Basic.
  - In the text file generated during `lcmexport`, comment all the import entries, except `import @Databases/Basic`.
  - Also comment `/Sample/Databases/Basic/Basic outline` under `@Databases/Basic`, just to import data alone.
  - Note that `-overwrite` option is not valid for this use case (“data only” import). The reason is that during import, LCM will drop the entire application and import it as blank. Then, only data is attempted to be imported, without the outline, therefore making the application invalid.
- **Import outline only**
  You want to update the Sample.Basic cube with just the outline from the exported zip.
  - In the `IMPORT` section at the end of the text file, comment all entries except "import @Databases/Basic".
  - Also comment "/Sample/Databases/Basic/Data" under "@Databases/Basic", just to import the outline.
- **Import single cube for an application with multiple cubes**

Sample application has three cubes named Basic, Basic1, Basic2, and you want to just import Basic.

- In the `IMPORT` section at the end of the text file, comment all entries except "Basic" cube (import @Databases/Basic, import @Databases/Basic/Xml_files, etc.).
- Without the `-overwrite` option, it imports or overrides only the Basic cube, whereas other cubes (Basic1, Basic2) in that application, remain as they are without any impact.
- With the `-overwrite` option, it drops and recreates the application, with just the Basic cube.

## Test the Migrated Essbase Instance

After migrating your Essbase instance, test thoroughly to ensure it's production-ready.

**Essbase post-migration tasks**:

- If you have any artifacts in LCM that are not supported for migration, they can be manually migrated.
- Test that data loads and dimension builds work as expected in migrated applications.
- Run a Smart View report to check connectivity and data.
- After the results look OK, scan the application logs for errors, warnings, and suspicious messages.

## Post Upgrade Tasks for CLI

After migrating or upgrading to Essbase 21c (Release 21.4 or higher), users of CLI must take the following actions, if applicable to their usage.

The Service Administrator needs to recreate any saved local connections that were created using the createlocalconnection command.

All affected CLI users must reset any stored passwords they created using the setpassword command.

## Migrate Multiple Essbase Instances to a Single Shared Services Instance

Here you can learn how to migrate multiple Essbase instances to a single Shared Services instance. When you have a large number of applications and using LCM is not feasible to export you applications, the following steps can be used.

> **Note:**
>
> This feature is available only for independent deployments.

### Back up multiple Essbase instances

To migrate, first do a backup of the instances.

1. Back up content of the source application directory.
2. Back up the source Essbase Relational Database Schema.
3. Back up EPM Shared Services assigned roles.

4. For all the above steps, see the instructions in Back Up Essbase: EPM Security Plus Shared Services Native Directory.

**Restore multiple Essbase instance to a single Shared Services instance**
Then do a restore of the instances.

1. Restore the <Application Directory> Folder Contents from the Source Backup into the Target Instance. See: Restore Essbase: EPM Security Plus Shared Services Native Directory.
2. Restore the Essbase Relational Database Schema. See: Restore Essbase: EPM Security Plus Shared Services Native Directory.

> **Note:**
>
> While restoring the Essbase Relational Database Schema, make sure dump file content matches the target cluster name, otherwise change it before importing.

# Upgrade Aggregate Storage Outline Version

These are the steps, for Linux and for Windows, to upgrade an aggregate storage outline to Essbase 21c.

> **Note:**
>
> Other references for ESSCMDQ workaround information are: How to Use ESSCMDQ to Compact Outlines (Doc ID 1534496.1) and Essbase 21c Compress Dimension Option Not Visible in JET UI (Doc ID 2853804.1).

**Server-based upgrade steps - for Linux**

1. Note that these steps can be performed only after importing the outline.
   a. Download platform-specific Essbase 21c ESSCMDQ from Download ESSCMDQ to your target Essbase system.
   b. Unzip the files directly to the same directory where ESSCMD is present in your installation.
   c. Make a copy of the existing script:

      ```
      ./Oracle/domains/esscs/esstools/bin/startESSCMD.sh
      ```

      as ESSCMDQ:

      ```
      ./Oracle/domains/esscs/esstools/bin/startESSCMDQ.sh
      ```

      Within this newly created script, change the call from:

      ```
      <Essbase_Product_Home>/products/Essbase/EssbaseServer/bin/startESSCMD.sh
      ```

to

```
<Essbase_Product_Home>/products/Essbase/EssbaseServer/bin/
startESSCMDQ.sh
```

d. Make a copy of the script:

```
<Essbase_Product_Home>/products/Essbase/EssbaseServer/bin/startESSCMD.sh
```

as:

```
<Essbase_Product_Home>/products/Essbase/EssbaseServer/bin/
startESSCMDQ.sh
```

e. Edit

```
<Essbase_Product_Home>/products/Essbase/EssbaseServer/bin/
startESSCMDQ.sh
```

and change the last line from

```
<EssbaseBasePath>/bin/ESSCMD
```

to:

```
<EssbaseBasePath>/bin/ESSCMDQ
```

f. Just before this last line, add the following lines:

```
export ESSCMDQ_UTF8MODE=1
export ESSLANG=.UTF-8@Binary
```

g. Create cube directory under the database directory.

```
mkdir $ARBORPATH/client/{appname}/{cubename}/cube
```

2. After launching this script:

```
<Essbase_Product_Home>/products/Essbase/EssbaseServer/bin/startESSCMDQ.sh
```

execute the following commands in ESSCMDQ:

```
#Login to Essbase 21c instance
login hostname username password;
#Download outline to client directory location.
qgetobject3 2 1 "appname" "cubename" "outlinename" $ARBORPATH/client/
{appname}/{cubename}/cube/{outlinename}.otl;
#Specify aggregate storage appname and cubename below
select "appname" "cubename";

#Update outline version
openotl 1 1 "appname" "cubename" "outlinename" "y" "y" 0;
```

```
setopgversion 0 "111241";
writeotl 0 "appname" "cubename" "outlinename"
lockobj 1 "appname" "cubename" "outlinename";
qPutObject3 2 1 "appname" "cubename" "outlinename" $ARBORPATH/client/
{appname}/{cubename}/cube/{outlinename}.otl N;
restructotl 1;
closeotl 0;
unlockobj 1 "appname" "cubename" "outlinename";
```

### Server-based upgrade steps - for Windows

1. Note that these steps can be performed only after importing the outline.
   a. Download platform-specific Essbase 21c ESSCMDQ from Download ESSCMDQ to your target Essbase system.
   b. Unzip the files directly to the same directory where ESSCMD is present in your installation.
   c. Make a copy of the existing script:

      ```
      .\Oracle\domains\esscs\esstools\bin\startESSCMD.bat
      ```

      as ESSCMDQ:

      ```
      .\Oracle\domains\esscs\esstools\bin\startESSCMDQ.bat
      ```

      Within this newly created script, change the call from:

      ```
      <Essbase_Product_Home>\products\Essbase\EssbaseServer\bin\startESSCMD.ba
      t
      ```

      to

      ```
      <Essbase_Product_Home>\products\Essbase\EssbaseServer\bin\startESSCMDQ.b
      at
      ```

   d. Make a copy of the script:

      ```
      <Essbase_Product_Home>\products\Essbase\EssbaseServer\bin\startESSCMD.ba
      t
      ```

      as:

      ```
      <Essbase_Product_Home>\products\Essbase\EssbaseServer\bin\startESSCMDQ.b
      at
      ```

   e. Edit

      ```
      <Essbase_Product_Home>\products\Essbase\EssbaseServer\bin\startESSCMDQ.b
      at
      ```

and change the last line from

```
"%ESSBASEPATH%\bin\ESSCMD.exe" %*
```

to:

```
"%ESSBASEPATH%\bin\ESSCMDQ.exe" %*
```

f. Just before this last line, add the following lines:

```
set ESSCMDQ_UTF8MODE=1
set ESSLANG=.UTF-8@Binary
```

g. Create cube directory under the database directory.

```
mkdir %ARBORPATH%\client\{appname}\{cubename}\cube
```

2. After launching this script:

```
<Essbase_Product_Home>\products\Essbase\EssbaseServer\bin\startESSCMDQ.bat
```

execute the following commands in ESSCMDQ:

```
#Login to Essbase 21c instance
login hostname username password;
#Download outline to client directory location.q
qgetobject3 2 1 "appname" "cubename" "outlinename" %ARBORPATH%/client/
{appname}/{cubename}/cube/{outlinename}.otl;
#Specify aggregate storage appname and cubename below
select "appname" "cubename";

#Update outline version
openotl 1 1 "appname" "cubename" "outlinename" "y" "y" 0;
setopgversion 0 "111241";
writeotl 0 "appname" "cubename" "outlinename"
lockobj 1 "appname" "cubename" "outlinename";
qPutObject3 2 1 "appname" "cubename" "outlinename" $ARBORPATH/client/
{appname}/{cubename}/cube/{outlinename}.otl N;
restructotl 1;
closeotl 0;
unlockobj 1 "appname" "cubename" "outlinename";
```

**Note:**

1. If you get the following error while running writeotl, it can be ignored.

   ```
   WriteOtl:
   Error: Invalid location => 0
   sts: 0
   ```

2. While executing “qgetobject3” command, you must provide the full path, which can be downloaded from server (Linux syntax).

   ```
   qgetobject3 2 1 asos Sample Sample /scratch/12cesscs/data/client/
   asos/Sample/Sample.otl
   ```

# Export Essbase 11g On-Premise Cubes

If you have applications and cubes that were created in a supported on-premises instance of Essbase, then you can use the 11g Excel Export Utility, which is a command-line tool, to export the metadata and data of a cube into an application workbook. Then you can import the application workbook to create a cube in the cloud service.

Using the 11g Excel Export Utility, you can export applications and cubes created in Essbase on-premises instances: 11.1.2.4.0nn, 11.1.2.4.5nn, 12.2.1, and later. You can't export cubes on these releases to application workbooks.

See:

- Download the 11g Excel Export Utility
- Review Member Names Before you Import an Application Workbook Created by the 11g Excel Export Utility

## Download the 11g Excel Export Utility

The cube export utility is supported on Windows and UNIX/Linux.

To download the 11g Excel Export Utility from Essbase:

1. In the Essbase web interface, on the Applications page, click **Console**.
2. On the Console page, click **Download**
   
   next to **11g Excel Export Utility.**
3. Save the 11g Excel Export Utility, which is named `dbxtool.zip`, to a local drive.

## Review Member Names Before you Import an Application Workbook Created by the 11g Excel Export Utility

When importing an application workbook that was created using the 11g Excel Export Utility, you should carefully review member names in the application workbook. Member names are exported to the application workbook as is. If a member name ends with a backslash (for example, mbrname\ or mbr\name\), then the member name is exported to the application workbook as is (mbrname\ or mbr\name\). During the import process, however, the trailing

backslash is interpreted as an escape character and the member is rejected (not added to the cube outline).

When the import process is completed, a dialog box provides status details, such as whether a dimension build was successful or if errors were encountered.

For each dimension in which one or more member names are rejected, an error file is created. The error file is named `err_DimName.txt` or `err_Dim_DimName.txt`. For example, if the Year dimension has any rejected member names, the error file name is `err_Year.txt` or `err_Dim_Year.txt`.

In the dimension error file, each rejected member name is listed, as shown:

```
\\Record #98 - Error in association transaction [RB6300] to [Curr_EUR] (3362)
"OTHER","RB6300","N","","","Ballsport L","","","","","Curr_EUR"
```

The rejected member record text files are available on the Files page. Review the text files and correct the issues in the application workbook.

8

# Manage Essbase User Roles and Application Permissions

Essbase integrates with security managed by Oracle to create a highly secure environment.

Now that you have migrated from Essbase 11g On-Premise to Essbase 21c, this section explains the user roles and application permissions that you use to manage access in your Essbase 21c application environment. The roles and permissions, and how you assign them, vary depending on the identity provider you selected for user authentication.

> **Note:**
>
> If you're managing user roles on Essbase 21c on Oracle Cloud Infrastructure via Marketplace, see: Manage Users and Roles in the Essbase Stack Deployment on OCI documentation.

If you're using Shared Services authentication,

1. Provision users and groups using the Shared Services Console in your target EPM Foundation-only instance that you have configured with Essbase 21c.
2. Use your existing Shared Services user and application roles, or map to the WebLogic roles in Essbase 21c.

If you're using WebLogic Embedded LDAP authentication (with or without federation to an external identity provider),

1. Provision users and groups using the Essbase web interface or REST API in your Essbase 21c platform.
2. Use the WebLogic roles in Essbase 21c.

**Topics:**



## WebLogic Security Users and Roles

There are three Essbase user roles if you choose WebLogic based security: User, Power User, and Service Administrator. Application permissions, granted separately, are Application Manager, Database Manager, Database Update, and Database Access.

The following are common use cases for assigning access to users using WebLogic security:

- Users can view and access cubes (databases) for which they were assigned access to the related applications.

- Power Users can create enterprise-level cubes and grant other users access to applications for which they have an Application Manager role.
- Service Administrators can assign users at all levels and manage all aspects of the applications, cubes, and users. Service Administrators can assign a Database Update role for users who need to update data in a cube.

To provide access to Essbase users, the following steps are required:

- Assign Essbase user role
- Assign Essbase application-level permissions

Administrators assign appropriate user/group roles and application permissions using the Essbase web interface or the REST API. User access permissions are described in Understand Your Access Permissions in Essbase, in the *Using Oracle Essbase* documentation.

## WebLogic Security User Roles and Application Permissions

Users can work with applications and cubes according to their assigned WebLogic roles and permissions. Roles and permissions help you manage the business activities users are permitted to perform within an Essbase instance, and the application data that they can access.

User roles are incremental; access granted to lower-level roles is inherited by higher-level roles. For example, Service Administrators, in addition to the access that only they have, inherit the access granted to Power User and User roles. You assign user roles in the Security page (available only to Service Administrators).

**Table 8-1 User Roles**

| User Role | Description |
|---|---|
| Service Administrator | Full access to administer users, applications, and cubes. |
| Power User | Has same permission as User Role, with added ability to create applications and cubes. Has Application Manager permission for the applications and cubes this user created, as well as the ability to delete them. Any additional permission must be granted, the same as for User Role. |
| User | Ability to access any provisioned application, or a cube that has a minimum access permission. This user role has no access to administrative tasks in applications or cubes unless that permission is granted at the application level. |

Users can access most Essbase features and functionality only after being assigned an application permission in addition to their user role. Application permissions determine more than simply which users and groups can see an application or cube. They also determine whether the user can view data, update data, or manage the cube or application.

Application permissions can be assigned to users and groups using the Permissions tab within the application inspector (available to Service Administrators, application managers, and some power users).

**Table 8-2 Application Permissions**

| Application Permission | Description |
|---|---|
| Application Manager | Ability to create, delete, and modify cubes and application settings within the assigned application; assign users to an application; create and delete scenarios, and give permission to run calculation scripts. |
| Database Manager | Ability to manage cubes, cube elements, locks, and sessions within the assigned application; create and delete scenarios, execute calculation scripts, and assign permissions to run calculation scripts. |
| Database Update | Ability to read, load, update, and clear data values based on assigned scope. Ability to create and delete scenarios. Ability to run provisioned calculation scripts. |
| Database Access | Ability to access scenarios, read data values in all cells, and access specific data and metadata, unless further overridden by filters. Can update values in specific cells, if granted write access to those cells through filters. |

## Provision Application Permissions

If you're a Service Administrator or Power User, you can provision application access permissions, which are incremental. Upper-level permissions include the privileges of lower-level permissions.

Users can have a unique permission for each application or cube. The permissions, from least privileged to highest, are:

- Database Access
- Database Update
- Database Manager
- Application Manager

To provision application roles using the Essbase web interface,

1. On the Applications page, select an application row, and then in the **Actions** menu, select **Inspect**.
2. On the **Permission** tab, use the + to open a menu for selecting users or groups to provision for access to the application.
3. Use the radio buttons to select the appropriate role(s) for the relevant users and groups.
4. Click **Close**.

# EPM Shared Services Security Users and Roles

All roles from EPM Shared Services can be mapped to the new roles and permissions, or you can to use those EPM Shared Services roles.

Essbase offers the following roles when using EPM Shared Services Security in the Essbase web interface.

**Table 8-3 Essbase Server Roles**

| Role | Description |
|---|---|
| Administrator | Full access to administer Essbase Server, applications, and databases. This is same as Service Administrator role in WebLogic Security mode. |
| Create/Delete Application | Creates and deletes applications and databases. Includes Application Manager and Database Manager permissions for the applications and databases created by this user.<br>This is same as 'Power User' role in WebLogic Security mode. |
| Server Access | Accesses any application or database belonging to this Essbase Server. This level is the minimum access permission a user must have to access applications and databases.<br>This is same as 'User' role in WebLogic Security mode. |
| Provisioning Manager | NA |

**Essbase Application Roles**

| Role | Description |
|---|---|
| Calc | Calculates, updates, and reads data values based on assigned scope, using any assigned calculations and filter<br>This is same as 'Database Update' role in WebLogic Security mode. |
| Filter | Accesses specific data and metadata according to filter restrictions |
| Application Manager | Creates, deletes, and modifies databases and application settings within the assigned application. Includes Database Manager permissions for databases within the application. An Application Managers can delete only those applications and databases that he created.<br>This is same as 'Application Manager' role in WebLogic Security mode. |
| Database Manager | Manages the databases, database artifacts, and locks within the assigned application<br>This is same as 'Database Manager' role in WebLogic Security mode. |
| Provisioning Manager | NA |

| | |
|---|---|
| Read | Reads data values<br><br>This is same as 'Database Access' role in WebLogic Security mode. |
| Write | Updates and reads data values based on assigned scope, using any assigned filter<br><br>This is similar to 'Database Update' role in WebLogic Security mode except user cannot perform calc/script execution. |
| Start/Stop Application | Starts and stops applications or databases |

# About Mapping Roles

Oracle Essbase offers a choice of mapping user roles. Here they are compared.

A common use case for migrating of user and group roles are when migrating from Essbase 11g On-Premise using EPM 11g to Essbase using EPM Shared Services. This requires no role mapping.

Role mapping is relevant when migrating from Essbase 11g On-Premise using EPM 11g to the target Essbase 21g security, using WebLogic Embedded LDAP.

**Table 8-4 Mapping Roles During Migration**

| Level | Source: 11g EPM Shared Services Security | Target: 21c WebLogic Embedded LDAP |
|---|---|---|
| Server | Server Access | User |
| Server | Provisioning Manager | - |
| Server | Create/Delete Application | Power User |
| Server | Administrator | Service Administrator |
| Application | Provisioning Manager | - |
| Application | Application Manager | Application Manager |
| Application | Database Manager | Database Manager |
| Application | Calc | Database Update |
| Application | Write | Database Update |
| Application | Read | Database Access |
| Application | Filter | Database Access |
| Application | Start/Stop Application | - |
| HSS | LCM Administrator | - |

9

# Manage Server Operations

Let's explore the processes to manage Essbase server operations.

**Topics:**



## Stop, Start, and Check Servers

Essbase platform components run as managed servers on a WebLogic application server. Start them all using `start.sh` or `start.cmd` in `esstools`. Stop them all using `stop.sh` or `stop.cmd`. You can also list the status, and start or stop individual server components.

For Linux, Essbase can be started using the startup script `start.sh`. Status can be checked using `status.sh`, and components can be stopped using `stop.sh`.

For Windows, Essbase can be started using the startup commands `start.cmd`. Status can be checked using `status.cmd`, and components can be stopped using `stop.cmd`.

These are located in the configuration directory of your domain, under esstools/bin.

- For Linux:

  ```
  <Domain_Home>/esstools/bin
  ```

- For Windows:

  ```
  <Domain_Home>\esstools\bin
  ```

### Check Managed Server Status

Run the status to see which managed servers are running in the Essbase platform:

- For Linux:

  ```
  <Domain_Home>/esstools/bin/status.sh
  ```

In this example, AdminServer and Essbase Server are shown in the script as running:

```
[/scratch/user/oracle_home/user_projects/domains/essbase_domain/esstools/
bin]$ ./status.sh
Domain status; Using domainHome:
/scratch/user/oracle_home/user_projects/domains/essbase_domain ...
Initializing WebLogic Scripting Tool (WLST) ...
Welcome to WebLogic Server Administration Scripting Shell
Type help() for help on available commands
Reading domain...
/Servers/AdminServer/ListenPort=7001
Accessing admin server using URL t3://myhost:7001
Server Name       Server Status   Type       Essbase Status
Machine
 ...........       ............   ....       ............   ...........

 AdminServer       RUNNING         Server     --
myhost.example.com
 essbase_server1   RUNNING         Server     Active
myhost.example.com
 eas_server1       --              Server     --
--
```

If the status fails with an error, for example, that the connection to Node Manager was refused, the log should be analyzed for the cause of the error.

- For Windows:

```
<Domain_Home>\esstools\bin\status.cmd
```

> **Note:**
>
> On your Windows machine, you can also check the status of Windows Services. In Windows Task Manager > Services, you can view Windows services that are running in the background.

**Start All Servers**

Run startup, without any arguments, to start Node Manager, all managed servers, and AdminServer, in the Essbase platform:

- For Linux:

```
<Domain_Home>/esstools/bin/start.sh
```

- For Windows:

```
<Domain_Home>\esstools\bin\start.cmd
```

The startup always starts WebLogic Node Manager. If no argument is specified to the startup script, as in the example above, Node Manager starts AdminServer, and AdminServer starts managed servers, including the Essbase server (and EAS server, if applicable).

Alternately, the startup can be used to start a particular server, if a server name argument is provided:

```
start.sh -i <server name>
```

If a server name is specified to the startup script, Node Manager starts the specified server only. For example, to start only the Essbase server,

- For Linux:

  ```
  ./start.sh -i essbase_server1
  ```

- For Windows:

  ```
  .\start.cmd -i essbase_server1
  ```

### Before stopping servers: prepare for shutdown

When you need to stop your Essbase services, consider the impact to active users. Enable/disable commands are available to allow you to prevent new connections, and you can write scripts using wait times to ensure that existing user operations have time to finish. If some operations are running for too long, you can terminate sessions and individual operations. Once all users are off the system, you can proceed to stop the services.

If you need to stop active user sessions, you can use the following workflow:

1. In the application settings, disable connections and commands (In MaxL, Alter Application **disable connects|commands**)
2. In the database settings, disable startup (In MaxL, Alter Database **disable startup**)
3. At the Essbase server level, log out all users from the system and terminate all active requests (In MaxL, Alter System **logout session** and **kill request**)
4. For each cube, verify that all sessions and requests are terminated (in MaxL, Display Session)
5. Shut down all the applications (in MaxL, Alter System **unload application**)

### Stop All Servers

Run the stop (Linux) script or (Windows) command, without any arguments, to stop Node Manager, AdminServer, and all managed servers in the Essbase platform:

- For Linux:

  ```
  <Domain_Home>/esstools/bin/stop.sh
  ```

- For Windows:

  ```
  <Domain_Home>\esstools\bin\stop.cmd
  ```

If a server name is specified to the stop (Linux) script or (Windows) command, Node Manager stops the specified server. For example, if you installed EAS server and don't need it running now, you can use:

```
./stop.sh -i eas_server1
```

### Start Secondary Managed Server when AdminServer is Not Available

When Essbase is configured for high availability, on the secondary (or any additional failover) node, if you need to start the WebLogic managed server when the primary node becomes unavailable, follow these instructions. Provide the managed server name of the secondary node, and the AdminServer URL, even though the AdminServer is unavailable. When prompted, also provide WebLogic administrator credentials.

1. SSH to the Essbase secondary node (Host 2).
2. Navigate to `<Domain Home>/bin`.
3. Run the script to start the WebLogic managed server, using the following syntax. You need to provide the AdminServer host name and the AdminServer port, even though AdminServer is not available.

   ```
   startManagedWebLogic.sh <failover-managed-server-name> t3(s)://
   <AdminServer-Host>:<AdminServer-Port>
   ```

   Linux Example with TLS/SSL:

   ```
   ./startManagedWebLogic.sh essbase_server2 t3s://adminserver:7002
   ```

   Linux Example without TLS/SSL:

   ```
   ./startManagedWebLogic.sh essbase_server2 t3://adminserver:7001
   ```

   Windows Example with TLS/SSL:

   ```
   .\startManagedWebLogic.cmd essbase_server2 t3s://adminserver:7002
   ```

   Windows Example without TLS/SSL:

   ```
   .\startManagedWebLogic.cmd essbase_server2 t3://adminserver:7001
   ```

### Stop Secondary Managed Server when AdminServer is Not Available

When Essbase is configured for high availability, on the secondary (or any additional failover) node, you can stop the WebLogic managed server independently, in case the primary node and AdminServer become unavailable.

1. SSH to the Essbase secondary node (Host 2).
2. Navigate to `<ORACLE_HOME>/oracle_common/common/bin`.
3. Run the WebLogic Scripting Tool.

   Linux example:

   ```
   ./oracle_common/common/bin/wlst.sh
   ```

   Windows example:

   ```
   .\wlst.cmd
   ```

4. At the `wls:/offline>` prompt, connect using the following syntax. You need to provide the WebLogic administrator credentials and the secondary (failover) host name and port.

   ```
   connect('<weblogic-admin-user>','<weblogic-admin-user-password>','t3(s)://
   <failover-managedServer-host>:<failover-managedServer-port>')
   ```

   Example with TLS/SSL:

   ```
   connect('WLadminusername','WLadminpassword','t3s://
   essbase_server.example.com:9001')
   ```

   Example without TLS/SSL:

   ```
   connect('WLadminusername','WLadminpassword','t3://
   essbase_server.example.com:9000')
   ```

5. Shut down the secondary (failover) host.

   Example:

   ```
   shutdown('essbase_server2','Server','true',1000, force='true',
   block='true')
   ```

6. Disconnect from the AdminServer.

   Example:

   ```
   disconnect()
   ```

7. Exit the WebLogic Scripting Tool.

   Example:

   ```
   exit()
   ```

**For Windows only - Start and Stop Essbase Service**

Windows SCM can be used to start or stop the Essbase service. To do this, open Windows SCM > select Essbase service > select and start or stop the service on Windows SCM.

**For Independent (On-Premise) deployments only - rotation of Essbase server logs**

For Independent (On-Premise) deployments, log rotation of `essbase_server1.out` is not supported and you must manually take a backup of the log file, when the servers are stopped. The file is located in `<DOMAIN_HOME>/<DOMAIN_NAME>/servers/essbase_server1/logs/`.

Backup saves older versions of the log, and should be done as the current log file size becomes very large.

# Patch and Roll Back

You can patch Oracle Essbase instances using the OPatch tool, which runs patches to a new version of binaries. You can also roll back an update, if necessary.

Rolling back from a patch to a version that's older than what was used to configure the Essbase instance is not supported.

> **Note:**
>
> If you created connections or Datasources after applying the patch, and then roll back the patch, you must re-create them. This step is required for drill through and other connection-dependent features to continue working as before.

> **Note:**
>
> After you roll back an OPatch, you may need to recreate transparent and replicated partitions, and re-validate the partitions.

> **Note:**
>
> When you need to upgrade Java from JDK 1.8.0_291 or higher to 1.8.0_331, see Upgrade Java after Configuration to JDK 1.8.0_331 or Higher.

**To install a software update (patch/upgrade) to an Essbase instance**

1. Stop all managed servers and system components, including Essbase Server, EAS Server, Admin Server, and Node Manager.

   For Linux:

   ```
   sh <Oracle_Home>/user_projects/domains/essbase_domain/esstools/bin/stop.sh
   ```

   For Windows:

   ```
   <Oracle_Home>\user_projects\domains\essbase_domain\esstools\bin\stop.cmd
   ```

   For an explanation of Oracle_Home, see Environment Locations in the Essbase Platform.

2. Check the build number.

   For Linux:

   ```
   cat <Oracle_Home>/essbase/bi-epm-registry/baseproperties/essbase/
   essbase_registry.properties
   ```

   For Windows (open essbase_registry.properties using Notepad):

   ```
   <oracle_home>\essbase\bi-epm-
   registry\baseproperties\essbase\essbase_registry.properties
   ```

3. Apply OPatch. You can apply it directly, while in zip format, providing the absolute path of the zip file. You can optionally unzip the file and apply the patch, providing the absolute path of the unzipped folder.

   a. Run the command. For example,

For Linux:

```
<Oracle_Home>/OPatch/opatch apply <Path of Linux opatch zip file>
```

For Windows:

```
<Oracle_Home>\OPatch\opatch apply <Path of Windows opatch zip file>
```

b. Check the build number.

For Linux:

```
cat <Oracle_Home>/essbase/bi-epm-registry/baseproperties/essbase/
essbase_registry.properties
```

For Windows (open essbase_registry.properties using Notepad):

```
<oracle_home>\essbase\bi-epm-
registry\baseproperties\essbase\essbase_registry.properties
```

4. Start all servers.

For Linux:

```
sh <Oracle_Home>/user_projects/domains/essbase_domain/esstools/bin/start.sh
```

For Windows:

```
<Oracle_Home>\user_projects\domains\essbase_domain\esstools\bin\start.cmd
```

**[Optional] Roll back update if necessary**

1. Stop the servers.
For Linux:

```
sh <Oracle_Home>/user_projects/domains/essbase_domain/esstools/bin/stop.sh
```

For Windows:

```
<Oracle_Home>\user_projects\domains\essbase_domain\esstools\bin\stop.cmd
```

2. Get the Unique OPatch ID.
For Linux:

```
<Oracle_Home>/OPatch/opatch lsinventory
```

For Windows:

```
<Oracle_Home>\OPatch\opatch lsinventory
```

3. Roll back the applied OPatch. The following sample syntax shows an OPatch ID example. Use the relevant OPatch ID.

For Linux:

```
<Oracle_Home>/OPatch/opatch rollback -id 3012639
```

For Windows:

```
<Oracle_Home>\OPatch\opatch rollback -id 3012639
```

4. Check the current build number.
For Linux:

```
cat <Oracle_Home>/essbase/bi-epm-registry/baseproperties/essbase/
essbase_registry.properties
```

For Windows (open essbase_registry.properties using Notepad):

```
<oracle_home>\essbase\bi-epm-
registry\baseproperties\essbase\essbase_registry.properties
```

5. Start the servers.
For Linux:

```
sh <Oracle_Home>/user_projects/domains/essbase_domain/esstools/bin/start.sh
```

For Windows:

```
<Oracle_Home>\user_projects\domains\essbase_domain\esstools\bin\start.cmd
```

# Upgrade Java after Configuration to JDK 1.8.0_331 or Higher

The following workaround assists you with upgrading Java, while performing an Essbase patch or upgrade.

This workaround applies when all of the following are true:

- Essbase release is 21.3 or earlier
- Essbase is configured in Secure Connection Mode
- Installation was performed on JDK 1.8.0_291 version or later, and JDK will be upgraded to 1.8.0_331 version or later
- TLS mode is used

**Edit server startup script on Essbase domain machine to add Java system property**

1. Stop Essbase services (see Stop, Start, and Check Servers).
2. On the machine in which Essbase is deployed, navigate to `<DOMAIN_HOME>/bin`.
3. Make a backup copy of `setStartupEnv.sh` (if you're using a Linux installation) or `setStartupEnv.cmd` (if using Windows).
4. Open the relevant StartupEnv script (for Linux or Windows installations) for editing.
5. Find the section associated with ESSBASE-MAN-SVR. The section begins with comment: `Startup parameters for STARTUP_GROUP ESSBASE-MAN-SVR`.

6. Append the line, which includes the following, to SERVER_SYSTEM_PROPERTIES:

```
-Dcom.sun.jndi.ldapURLParsing=LEGACY
```

Example of Linux file **<DOMAIN_HOME>/bin/setStartupEnv.sh** is shown below. The added line is shown in bold:

```
# Startup parameters for STARTUP_GROUP ESSBASE-MAN-SVR
if [ "${STARTUP_GROUP}" = "ESSBASE-MAN-SVR" ] ; then
# Java system properties.
      SERVER_SYSTEM_PROPERTIES="-Dopss.version=12.2.1.3 -
Digf.arisidbeans.carmlloc=${ORACLE_DOMAIN_CONFIG_DIR}/carml -
Digf.arisidstack.home=${ORACLE_DOMAIN_CONFIG_DIR}/arisidprovider -
Doracle.security.jps.config={DOMAIN_HOME}/config/fmwconfig/jps-config.xml -
Doracle.deployed.app.dir=${DOMAIN_HOME}/servers/${SERVER_NAME}/tmp/
_WL_user -Doracle.deployed.app.ext=/- -Dweblogic.alternateTypesDirectory=$
{COMMON_COMPONENTS_HOME}/modules/oracle.ossoiap,{COMMON_COMPONENTS_HOME}/
modules/oracle.oamprovider,${COMMON_COMPONENTS_HOME}/modules/oracle.jps -
Doracle.mds.filestore.preferred=${ORACLE_FORCE_MDS_FILESTORE} -
Dadf.version=12.2.1.3.0 -Dweblogic.jdbc.remoteEnabled=true -
common.components.home=${COMMON_COMPONENTS_HOME} -Djrf.version=12.2.2 -
Dorg.apache.commons.logging.Log=org.apache.commons.logging.impl.Jdk14Logger
 -Ddomain.home=${DOMAIN_HOME} -
Doracle.server.config.dir={ORACLE_DOMAIN_CONFIG_DIR}/servers/$
{SERVER_NAME} -Doracle.domain.config.dir=${ORACLE_DOMAIN_CONFIG_DIR} -
Dessbase.oracle.home=${ESSBASE_PRODUCT_HOME} -DESS_ES_HOME=${DOMAIN_HOME}/
servers/${SERVER_NAME}/aps -Daps.property.file={DOMAIN_HOME}/config/
fmwconfig/essconfig/aps/essbase.properties -DESSCS_12C=true -
Doracle.bi.12c=true -DESSBASEPATH=${ESSBASE_PRODUCT_HOME}/products/Essbase/
EssbaseServer -DARBORPATH=${ARBORPATH} -
DESSBASE_CONFIG_PATH={ESSBASE_CONFIG_PATH} -DODBCINI=${DOMAIN_HOME}/config/
fmwconfig/essconfig/core/odbc.ini -DODBCINST=${DOMAIN_HOME}/config/
fmwconfig/essconfig/core/odbcinst.ini -
Dweblogic.security.SSL.minimumProtocolVersion=TLSv1 -
weblogic.security.SSL.hostnameVerifier=weblogic.security.utils.SSLWLSWildca
rdHostnameVerifier -DBI_ORACLE_HOME=${ESSBASE_PRODUCT_HOME} -
Dessbase.datasource=essbase_datasource -Djava.awt.headless=true -
Dcom.sun.jndi.ldapURLParsing=LEGACY -
Dhttp.keepAliveCache.socketHealthCheckTimeout=1 -
Dweblogic.security.SSL.ignoreHostnameVerification=true -
DODBC_URL='OCI;SERVICE=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
(HOST=myserver.example.com)(PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=orclpdb.myserver.example.com)))' -
DDISCOVERY_URL=https://myserver.example.com:9001/essbase/agent "
 export SERVER_SYSTEM_PROPERTIES="$SERVER_SYSTEM_PROPERTIES -
Dcom.sun.jndi.ldapURLParsing=LEGACY"
```

Example of Windows file **<DOMAIN_HOME>\bin\setStartupEnv.cmd** is shown below. Add a variable to SERVER_SYSTEM_PROPERTIES as below in bold:

```
@REM Startup parameters for STARTUP_GROUP ESSBASE-MAN-SVR
if %STARTUP_GROUP%==ESSBASE-MAN-SVR (
          @REM Java system properties.
set SERVER_SYSTEM_PROPERTIES=-Dopss.version=12.2.1.3 -
Digf.arisidbeans.carmlloc=%{ORACLE_DOMAIN_CONFIG_DIR}/carml -
```

```
Digf.arisidstack.home=%{ORACLE_DOMAIN_CONFIG_DIR}/arisidprovider -
Doracle.security.jps.config={DOMAIN_HOME}/config/fmwconfig/jps-config.xml -
Doracle.deployed.app.dir=%{DOMAIN_HOME}/servers/%{SERVER_NAME}/tmp/
_WL_user -Doracle.deployed.app.ext=/- -Dweblogic.alternateTypesDirectory=%
{COMMON_COMPONENTS_HOME}/modules/oracle.ossoiap,{COMMON_COMPONENTS_HOME}/
modules/oracle.oamprovider,%{COMMON_COMPONENTS_HOME}/modules/oracle.jps -
Doracle.mds.filestore.preferred=%{ORACLE_FORCE_MDS_FILESTORE} -
Dadf.version=12.2.1.3.0 -Dweblogic.jdbc.remoteEnabled=true -
common.components.home=%{COMMON_COMPONENTS_HOME} -Djrf.version=12.2.2 -
Dorg.apache.commons.logging.Log=org.apache.commons.logging.impl.Jdk14Logger
 -Ddomain.home=%{DOMAIN_HOME} -
Doracle.server.config.dir={ORACLE_DOMAIN_CONFIG_DIR}/servers/%
{SERVER_NAME} -Doracle.domain.config.dir=%{ORACLE_DOMAIN_CONFIG_DIR} -
Dessbase.oracle.home=%{ESSBASE_PRODUCT_HOME} -DESS_ES_HOME=%{DOMAIN_HOME}/
servers/%{SERVER_NAME}/aps -Daps.property.file={DOMAIN_HOME}/config/
fmwconfig/essconfig/aps/essbase.properties -DESSCS_12C=true -
Doracle.bi.12c=true -DESSBASEPATH=%{ESSBASE_PRODUCT_HOME}/products/Essbase/
EssbaseServer -DARBORPATH=%{ARBORPATH} -
DESSBASE_CONFIG_PATH={ESSBASE_CONFIG_PATH} -DODBCINI=%{DOMAIN_HOME}/config/
fmwconfig/essconfig/core/odbc.ini -DODBCINST=%{DOMAIN_HOME}/config/
fmwconfig/essconfig/core/odbcinst.ini -
Dweblogic.security.SSL.minimumProtocolVersion=TLSv1 -
weblogic.security.SSL.hostnameVerifier=weblogic.security.utils.SSLWLSWildca
rdHostnameVerifier -DBI_ORACLE_HOME=%{ESSBASE_PRODUCT_HOME} -
Dessbase.datasource=essbase_datasource -Djava.awt.headless=true -
Dcom.sun.jndi.ldapURLParsing=LEGACY -
Dhttp.keepAliveCache.socketHealthCheckTimeout=1 -
Dweblogic.security.SSL.ignoreHostnameVerification=true -
DODBC_URL='OCI;SERVICE=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
(HOST=myserver.example.com)(PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=orclpdb.myserver.example.com)))' -
DDISCOVERY_URL=https://myserver.example.com:9001/essbase/agent
-Dcom.sun.jndi.ldapURLParsing=LEGACY
@REM Java protocol handlers.
set JAVA_OPTIONS=%JAVA_OPTIONS% -
Djava.protocol.handler.pkgs=oracle.mds.net.protocol
```

7. Save `setStartupEnv.sh` or `setStartupEnv.cmd`.
8. Restart Essbase services. See Stop, Start, and Check Servers.
9. Log in to Essbase web interface to ensure you can access the instance.

# Unconfigure and Uninstall Essbase

Do the following steps to unconfigure and uninstall Essbase.

**Workflow and Prerequisites**

- When you want to unconfigure and uninstall Essbase, it's recommended to first perform unconfigure, and then to perform the uninstall command.
- For Windows platform: you must run command `sc delete EssbaseService` at Windows command prompt to re-install or re-configure Essbase if you had previously configured Essbase with Windows Service option enabled.
- Oracle Essbase must be present on your system before you drop a schema.

### Unconfigure Essbase

1. Perform a backup. See Back Up and Restore Essbase.
2. Stop all servers - Essbase Server, Admin Server, and EAS Server (if installed):

   **For Linux:**

   ```
   <Domain_Home>/esstools/bin/stop.sh
   ```

   If you encounter any problems with stopping a server, use the relevant process below (for Linux).

   - Stop Essbase Server:

     ```
     #
           ESSBASE_PID = ‘ps-ef | grep essbase_server_name | | grep -v grep
     | awk '{print $2}'
           ’kill -9  $ESSBASE_PID
     ```

   - Stop AdminServer:

     ```
     # ADMIN_SERVER_PID = ‘ps -ef | grep
           AdminServer | grep -v grep | awk '{print $2}' ‘kill -9 $
           ADMIN_SERVER_PID
     ```

   - Stop EAS Server:

     ```
     # EAS_SERVER_PID= ‘ ps -ef | grep
           eas_server_name | grep -v grep | | awk '{print $2}' ’
                       # kill -9
           $EAS_SERVER_PID
     ```

     For more information, see Stop, Start, and Check Servers.

   **For Windows:**

   ```
   <Domain_Home>\esstools\bin\stop.cmd
   ```

   Alternatively, you can open Task Manager > check for Essbase process (Process/Image Name is java.exe) > if any process is still present, stop them in Task Manager’s process list (by right-clicking on the process and select “End Process”).
3. Drop all RCU schemas, prefixes, and components, using the interface-based procedure or Silent mode, as described in Delete RCU Schemas for Essbase.
4. Delete the domain directory and application location (ARBORPATH directory), or use different directories in your next installation.

   ```
   # rm -rf  <Domain_Name>
   ```

   The paths can be obtained from the `config.rsp` (response file) generated during Essbase configuration. Before deleting, ensure that you backed up the application directory.
5. If you have the feature.txt file in your Oracle_Home directory, you must delete its directory now, before you run uninstall.

   After you're run the above steps, you can proceed to run uninstall.

**Uninstall Essbase**
There are optional arguments that you can enter on the command line, when you launch the installer to uninstall Essbase. See Installer Options - Syntax and Commands.

The uninstall process deletes binary directories and inventory entries created during installation. This process only installs Essbase and doesn't uninstall Fusion Middleware.

- **To uninstall using Silent mode**: Run the following command to uninstall the Essbase instance. If you want to uninstall all distributions (Essbase and FMW), replace the distributionName parameter value `essbase` with `all`.

  For Linux:

  ```
  <Oracle_Home>/oui/bin/deinstall.sh -silent -distributionName essbase
  ```

  For Windows:

  ```
  <Oracle_Home>\oui\bin\deinstall.cmd -silent -distributionName essbase
  ```

- **To uninstall using the interface procedure**: Run the command below, select the specific distribution (Essbase instance) to uninstall, and click **Uninstall**. Essbase Installer opens, runs uninstall tasks, and then displays a summary page for you to confirm by clicking **Uninstall**. Click **Finish** when done.

  For Linux:

  ```
  <Oracle_Home>/oui/bin/deinstall.sh
  ```

  For Windows:

  ```
  <Oracle_Home>\oui\bin\deinstall.cmd
  ```

# Change Password Policy

You can customize the password policy applied to new users created in the service or when resetting passwords.

This is only applicable for WebLogic Embedded LDAP mode, and for Oracle customer managed.

1. Connect to the Essbase service instance using Secure Shell (SSH) client software.
2. Switch to the Oracle user using the following:

   ```
   sudo su - oracle
   ```

3. Edit the policy file, in the Essbase service instance, as follows:

   ```
   vi /u01/data/domains/esscs/config/fmwconfig/essconfig/essbase/essbase-
   password-validation-rules.xml
   ```

   The following is the current default policy file:

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <essbase-password-validation-rules>
   ```

```
<cannot-contain-spaces>true</cannot-contain-spaces>
<cannot-contain-username>true</cannot-contain-username>
<maximum-password-length>20</maximum-password-length>
<minimum-alphabetic-chars>0</minimum-alphabetic-chars>
<minimum-password-length>8</minimum-password-length>
<minimum-lowercase-chars>0</minimum-lowercase-chars>
<minimum-numeric-chars>0</minimum-numeric-chars>
<minimum-special-chars>0</minimum-special-chars>
<minimum-uppercase-chars>0</minimum-uppercase-chars>
</essbase-password-validation-rules>
```

4. Exit from the editor using the following:

   ```
   :wq
   ```

   If you modify the policy file, it is dynamically updated, and you do not need to restart the service.

# Change WebLogic Password

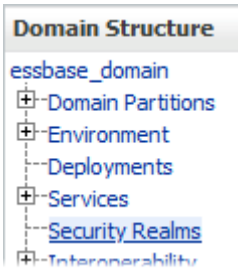
Use the WebLogic Server Administration Console to change your password for the WebLogic administrator account that you use to manage your Oracle Essbase and middleware servers.

1. Log in to the WebLogic Server Administration Console. The URL is of the format `<host>:<WL_adminserver_port>/console`.

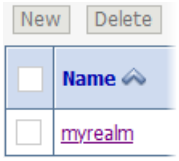
   Example of console URL for secure/TLS mode: `https://myserver.example.com:7002/console`

   Example of console URL for non secure mode: `http://myserver.example.com:7001/console`

2. On the home page, under **Domain Structure**, select **Security Realms**.



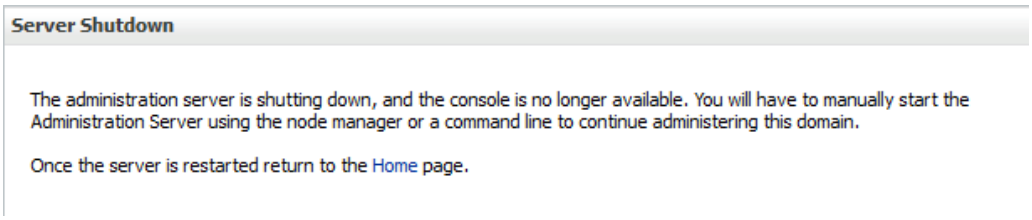

3. Under **Summary of Security Realms** > **Realms**, click the name **myrealm**.




4. Under **Settings for myrealm**, select the **Users and Groups** tab.
5. Under **Users**, click the WebLogic administrator's user name; for example, click **weblogic**.
6. Under **Settings for *administrator_name***, select the **Passwords** tab.

7. Enter the new password twice, and then click **Save**.
8. Restart all managed servers:
   a. On the home page, under **Environment**, select **Servers**.
   b. On the right pane, under **Summary of Servers**, click the **Control** tab.
   c. Select all servers from the check box, and select **Shutdown > Force shutdown now**.
   d. Click Yes to confirm.

      The server shutdown message displays.




9. **ssh** to the Essbase Server host.
10. Restart Essbase, as described in Stop, Start, and Check Servers. You'll be prompted for the WebLogic administrator user name and changed password during startup, and your changed password will be registered in the appropriate boot.properties file.

# Reset Essbase Repository Database Schema Passwords

If the Essbase Repository Database Schemas (RCU) passwords expired, you must change them and restart the services before you can use Essbase.

To determine whether problems with Essbase are caused by expired RCU passwords,

1. Navigate to `<Domain Home>/servers/<Essbase-Managed-Server-Name>/logs`.

   For an explanation of <*Domain Home*> and any other path/location variables referenced in this topic, see Environment Locations in the Essbase Platform.

   Linux example:

   ```
   cd <Domain Root>/essbase_domain/servers/essbase_server1/logs
   ```

   Windows example:

   ```
   chdir <Domain Root>\essbase_domain\servers\essbase_server1\logs
   ```

2. Check the log file `<Essbase-Managed-Server-Name>.out` for any Oracle Database password errors.

   Linux example:

   ```
   cat essbase_server1.out | grep password
   ```

   On Windows, open the log file and perform a search for `password`.

If you find errors similar to the following, you likely need to update expired RCU passwords.

```
Attempt to connect to OCI failed. [ORA-28002: the password will expire
within 3 days
```

To update expired RCU passwords,

1. Locate the schema name prefix (you can find it in `rcu.log`, created during configuration). For example, let's assume the schema prefix to be ABC123.
2. Using a client tool such as Oracle SQL Developer, and connecting as an administrative user with the privileges to change other users' passwords, log in to the RCU schema database.
3. Unlock the RCU schemas by executing the following SQL statements. In the examples below, replace the example password with the new password of the RCU schemas.

```
ALTER USER ABC123_MDS IDENTIFIED BY PPAASSWW ACCOUNT UNLOCK;
ALTER USER ABC123_IAU IDENTIFIED BY PPAASSWW ACCOUNT UNLOCK;
ALTER USER ABC123_IAU_APPEND IDENTIFIED BY PPAASSWW ACCOUNT UNLOCK;
ALTER USER ABC123_IAU_VIEWER IDENTIFIED BY PPAASSWW ACCOUNT UNLOCK;
ALTER USER ABC123_OPSS IDENTIFIED BY PPAASSWW ACCOUNT UNLOCK;
ALTER USER ABC123_STB IDENTIFIED BY PPAASSWW ACCOUNT UNLOCK;
ALTER USER ABC123_WLS IDENTIFIED BY PPAASSWW ACCOUNT UNLOCK;
ALTER USER ABC123_WLS_RUNTIME IDENTIFIED BY PPAASSWW ACCOUNT UNLOCK;
ALTER USER ABC123_ESSBASE IDENTIFIED BY PPAASSWW ACCOUNT UNLOCK;
```

4. Using SSH to the Essbase server machine, stop the server (all servers including AdminServer).

   Linux example:

   ```
   <Domain Home>/esstools/bin/stop.sh
   ```

   Windows example:

   ```
   <Domain Home>\esstools\bin\stop.cmd
   ```

5. If any Java process is running, stop the process. To find out if a Java process is running, you can use Task Manager on Windows, or on Linux, grep the process listing.

   Linux example:

   ```
   ps -eaf | grep javaI
   ```

6. Navigate to *<Domain Home>* and find the location of the Java Policy Store file, `jps-config.xml`.

   Linux example:

   ```
   cd <Domain Root>/essbase_domain
   find . -name jps-config.xml
   ```

   The file path returned should be: `<Domain Home>/config/fmwconfig/jps-config.xml`

Windows example:

```
chdir <Domain Root>\essbase_domain
dir "jps-config.xml" /s
```

The file path returned should be: `<Domain Home>\config\fmwconfig\jps-config.xml`. Save this information for the WebLogic Scripting Tool steps to follow.

7. Run the WebLogic Scripting Tool, located in `<ORACLE_HOME>/oracle_common/common/bin`.

   Linux example:

   ```
   <ORACLE_HOME>/oracle_common/common/bin/wlst.sh
   ```

   Windows example:

   ```
   <ORACLE_HOME>\oracle_common\common\bin\wlst.cmd
   ```

8. At the `wls:/offline>` prompt, update boot strap credentials, providing as arguments: the path to the Java Policy Store, the OPSS schema name, and a new RCU schema password.

   Note that `PPAASSW2` is shown here as an example of the new RCU schema password.

   Linux example:

   ```
   modifyBootStrapCredential(jpsConfigFile='<Domain Root>/essbase_domain/
   config/fmwconfig/jps-
   config.xml',username='ABC123_OPSS',password='PPAASSW2')
   ```

   Windows example:

   ```
   modifyBootStrapCredential(jpsConfigFile='<Domain
   Root>\essbase_domain\config\fmwconfig\jps-
   config.xml',username='ABC123_OPSS',password='PPAASSW2')
   ```

   The displayed warning shown below can be ignored.

   ```
   WARNING: Bootstrap services are used by OPSS internally and clients should
   never need to directly read/write bootstrap credentials. If required, use
   Wlst or configuration management interfaces.
   ```

9. Start Essbase Admin Server.

   Linux example:

   ```
   <Domain Home>/esstools/bin/start.sh -i AdminServer
   ```

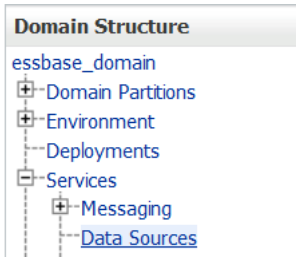
   Windows example:

   ```
   <Domain Home>\esstools\bin\start.cmd -i AdminServer
   ```

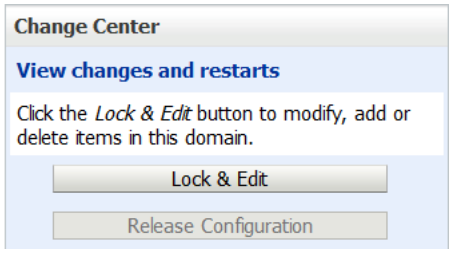
   See also Stop, Start, and Check Servers.

10. As the WebLogic administrator, log in to WebLogic Server Administrative console `http(s)://<hostname>:<admin server port>/console`, and update all Data Source passwords with the new password. You can use the same password for all schemas.

    a. From WebLogic console, under **Domain Structure**, navigate to **Services** > **Data Sources**.

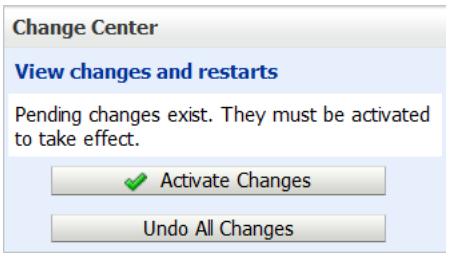



    b. In Change Center, click **Lock & Edit**.




    c. For each Data Source in the table, click the Data Source name, click the **Connection Pool** tab, update the **Password** and **Confirm Password** fields with the new password, and click **Save**.

    d. After all Data Source passwords have been updated and saved, click **Activate Changes** in the Change Center.




    e. Log out of the WebLogic console.

11. Using SSH to the Essbase server machine, once again run the WebLogic Scripting Tool, located in `<ORACLE_HOME>/oracle_common/common/bin`.

    Linux example:

```
<ORACLE_HOME>/oracle_common/common/bin/wlst.sh
```

Windows example:

```
<ORACLE_HOME>\oracle_common\common\bin\wlst.cmd
```

12. At the `wls:/offline>` prompt, log in to the AdminServer using WLST `connect`.

    Secure (TLS/SSL) mode example:

    ```
    connect('WLuser','WLpasswd','t3s://hostname.example.com:7001')
    ```

    Non-TLS mode example:

    ```
    connect('WLuser','WLpasswd','t3://hostname.example.com:7001')
    ```

13. At the `wls:/essbase_domain/serverConfig/>` prompt, update the credentials for Essbase schema user ABC123_ESSBASE using WLST `updateCred`, providing the new password.

    Example:

    ```
    updateCred(map='oracle.essbase',key='datasource.essbase',user='ABC123_ESSBA
    SE',password='PPAASSW2')
    ```

14. Disconnect from the AdminServer.

    Example:

    ```
    disconnect()
    ```

15. Exit the WebLogic Scripting Tool.

    Example:

    ```
    exit()
    ```

16. Using SSH to the Essbase server machine, stop and restart all Essbase services. See Stop, Start, and Check Servers.
17. Check that you can log in to Essbase.

# Use Essbase Administration Services Lite

You can optionally manage applications using Essbase Administration Services (EAS) Lite.

Although the Essbase web interface is the modern administration interface that supports all current platform features, a lite version of Essbase Administration Services is a limited-support option for continued management of your applications if your organization isn't ready to adopt the new interface. This option is available only for Essbase 21c independent installations of Essbase.

EAS Lite supports only features and functionality available in 11g, and not features added in later Essbase releases.

- Select to Include EAS Lite as a Managed Server
- Access the EAS Lite Console
- Access the EAS Lite Web Console
- Manage Applications Using EAS Lite

- Limitations of EAS Lite
- Limitations of Essbase web interface for EAS-Managed Applications
- View Application and Agent Logs in EAS Lite

### Select to Include EAS Lite as a Managed Server

When you configure Essbase, during the configuration of WebLogic server ports, you can optionally select a check box to enable EAS. This deploys both EAS and Essbase as WebLogic managed servers.

If you configured to include EAS Lite, then running `status.sh` (or `status.cmd`) for your Essbase services shows the AdminServer, Essbase server, and EAS server as RUNNING, SHUTDOWN, or FAILED. The following example is on Linux.

```
[/scratch/username/essbase21c/config/domains/essbase_domain/esstools/bin]$ ./
status.sh
Domain status; Using domainHome: /scratch/username/essbase21c/config/domains/
essbase_domain ...
Initializing WebLogic Scripting Tool (WLST) ...
Welcome to WebLogic Server Administration Scripting Shell
Type help() for help on available commands
Reading domain...
/Servers/AdminServer/ListenPort=7001
Accessing admin server using URL t3://myhost:7001
 Server Name       Server Status   Type     Essbase Status
Machine
 ...........       ............   ....     ............   ...........

 AdminServer       RUNNING         Server   --
myhost.example.com
 essbase_server1   RUNNING         Server   Active
myhost.example.com
 eas_server1       RUNNING         Server   --              myhost.example.com
```

### Access the EAS Lite Console

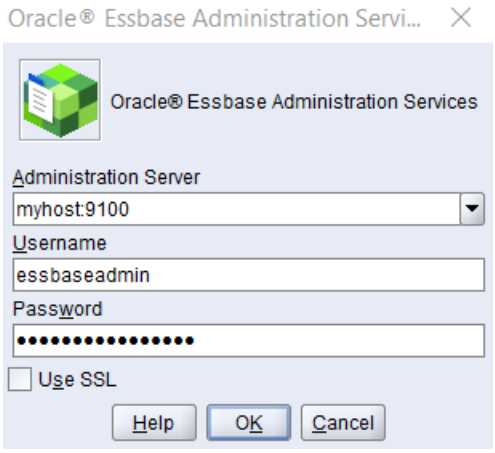
You can download and install EAS Lite for Windows, and alternatively access it using a web console.

You can also work on your EAS-managed application in MaxL, ESSCMD, and software developed using APIs.

### To install EAS Lite on Windows

1. If an older version of Essbase Administration Services Console is already installed, uninstall it. You must use the latest version, downloaded from the Essbase web interface. Previously downloaded versions may not work correctly.
2. Ensure that Oracle Java 8 is installed. You can get it from https://www.oracle.com/java/technologies/javase/javase-jdk8-downloads.html.
3. From the Essbase web interface, click **Console**, expand **Essbase Administration**, and download Essbase Administration Services Console to a local directory.
4. Extract `EASConsole.zip`, and double-click `EASConsole.exe` to extract and run the installer.
5. When the installation is complete, launch the Essbase Administration Services Console from Start Menu > Oracle Essbase > Start Administration Services Console.

6. Log in.

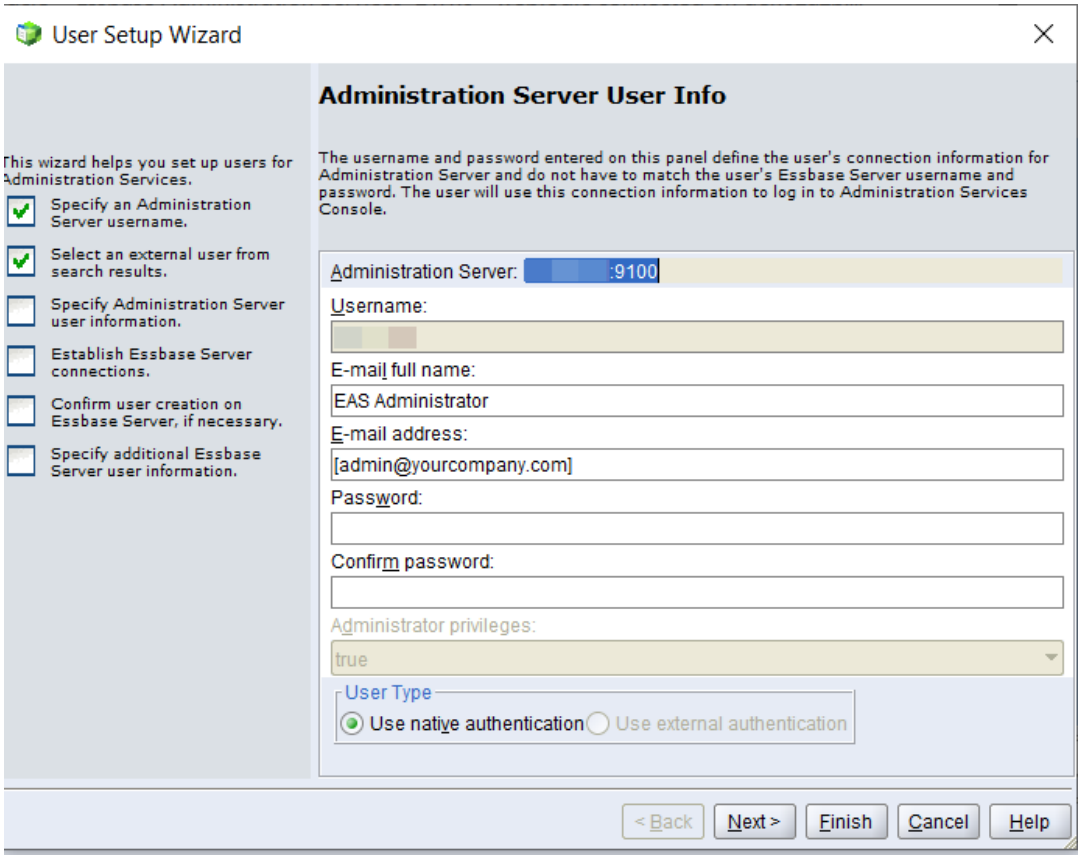



   a. For **Administration Server**, enter *hostname*:*port*, where the host name is the machine where EAS managed server runs, and the port number is what you configured for the EAS managed server when you ran Essbase Configuration Tool. If you enabled secure mode, the default port isn't 9100.

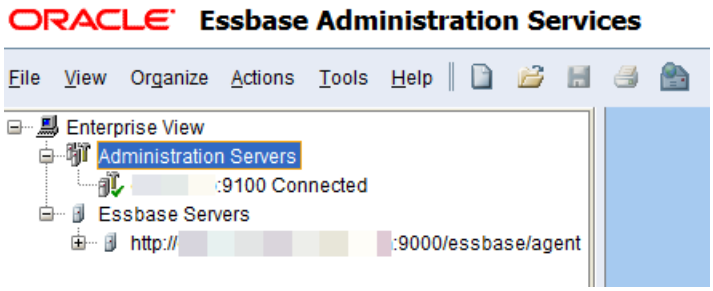
   b. For **Username** and **Password** enter your Essbase administrator credentials.

   c. Click **OK**.

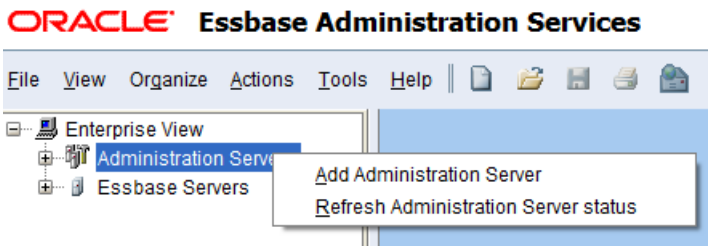
7. On the **Administration Server User Info** page, enter the e-mail information, re-enter your Essbase administrator password, and click **Next**. (No separate Administration Server user name is required).




8. On the **Essbase Server Connection** page, enter the fully qualified host name and port of your Essbase managed server (for example, `http://myhost.example.com:9000`), and enter the Essbase administrator credentials. Click **Set** and click **Next**.
9. Confirm if prompted, and click **Finish**. If the setup was successful, you should see a connected Administration Server and a corresponding, connected Essbase server.




10. If you expand the Essbase server and there are no applications displayed, you still need to set up an EAS managed application using the Essbase web interface. See *Manage an Application Using EAS Lite* section below.
11. If you have additional Essbase servers, you can also enter information for them:
    a. Add an additional Administration Server by right-clicking Administration Servers under Enterprise View.




b. Enter the Essbase server connection information.

You can add one Essbase server per Administration Server. Only one can be connected at a time.

### Access the EAS Lite Web Console

1. Open a web browser and navigate to the URL of the EAS managed server. For example,

   `http://hostname.example.com:9100/easconsole`

   Port numbers are configurable in the Essbase Configuration Tool, so the port number for your URL may be different. If you enabled secure mode, the default port isn't 9100.
2. Click **Launch**. If the EAS Lite console doesn't launch, you may need to configure your browser with a Java Web Start (javaws) plugin that can launch .jnlp files.

> **Tip:**
>
> You may need to use an older browser. Also, if your Essbase deployment is Windows Server 2022, see EAS Lite Troubleshooting.

### If Using TLS Everywhere and EAS Lite

Before you can log in from the EAS Lite web console, you need to import a certificate to the Java trust store. Do the following steps on the machine from which you will access the web console.

1. Export a self-signed certificate from the web browser.
   a. In the browser address bar, go to the EAS Lite **https** web console URL.
   b. To the left of the URL address, click the security alert icon (these vary by browser).
   c. Download or copy the certificate to a file (instructions vary by browser).
   d. Export the certificate to the file system.
2. Find the Java trust store by checking the value of the following option in `admincon.bat`:

   ```
   -Djavax.net.ssl.trustStore=%JAVA_HOME%\lib\security\cacerts
   ```

3. Import the certificate to the trust store.

   For example, for Java keytool,

   a. Set JAVA_HOME and PATH variables to indicate the correct version of Java that you installed locally or on another volume. The following example is for the bash shell on

Linux, and persists only for the current shell. If you want the settings to persist longer, you can add the export statements to your bash configuration file, `.bashrc`.

```
export JAVA_HOME=/usr/bin/java
export PATH=$JAVA_HOME/bin:$PATH
```

b. Import the certificate to the trust store. For example, on Windows,

```
keytool.exe -import -trustcacerts -keystore "C:\Program
Files(x86)\Java\jre1.8.0_241\lib\security\cacerts" -alias
"my01certificate" -file D:\my01elc.cer
```

If you are prompted for a password after issuing the command, enter your new password.

4. To check if the certificate was added, use the keytool list option to search based on alias. For example, on Windows,

```
keytool.exe -list -keystore "C:\Program
Files(x86)\Java\jre1.8.0_241\lib\security\cacerts" | findstr "my01"
```

### Manage Applications Using EAS Lite

Before you can connect to an application in EAS Lite, you must set it as an EAS managed application.

> **Note:**
>
> To set an application as EAS managed, during Essbase configuration of WebLogic server ports, **Enable EAS** must have been checked.

To manage an application using EAS Lite in the Essbase web interface,

1. Log in to the Essbase web interface.

   In the Redwood Interface,

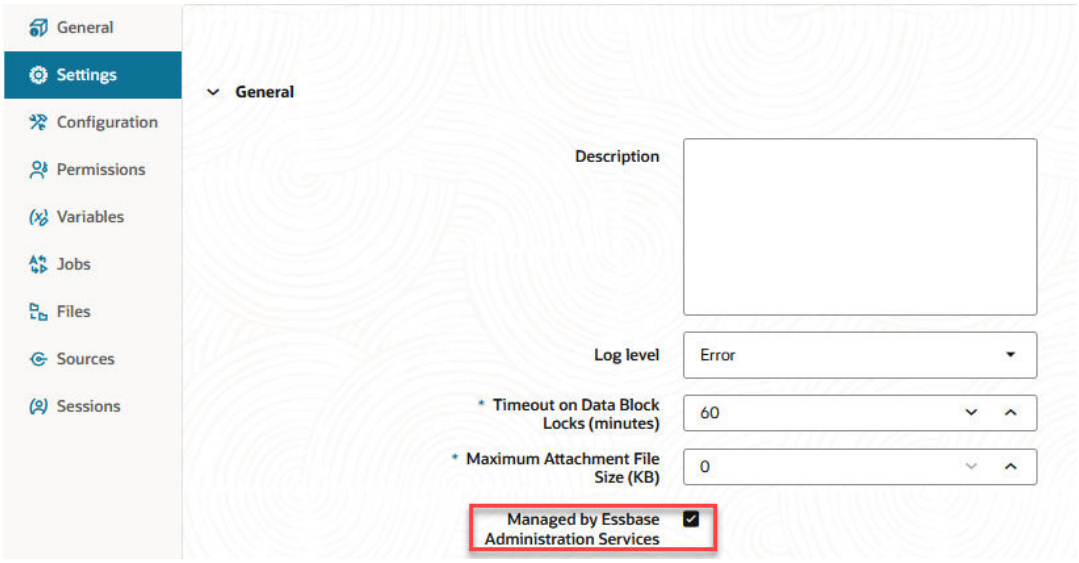
   a. Open the application.

   b. Click **Settings**, and select **Managed by Essbase Administration Services**.

   In the Classic Web Interface,

   a. From the Actions menu to the right of the application name, launch the inspector, and click **Settings**.

   b. From the **General** tab, select **Managed by Essbase Administration Services**.

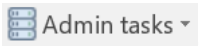


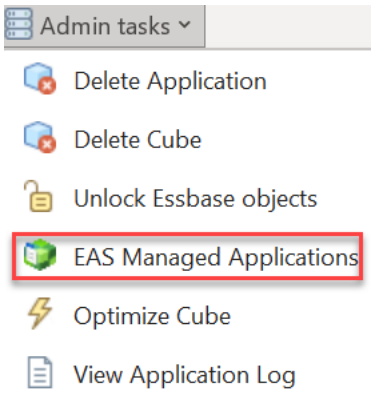

2. Click **Save**, **OK**, and **Close**.

If you decide to try managing the application fully in the Essbase web interface, instead of using EAS Lite, you can unselect the **Managed by Essbase Administration Services** option from the application general settings.

> **Caution:**
>
> This action is irreversible for the current application. It's recommended to back up the EAS-managed application before implementing this action.

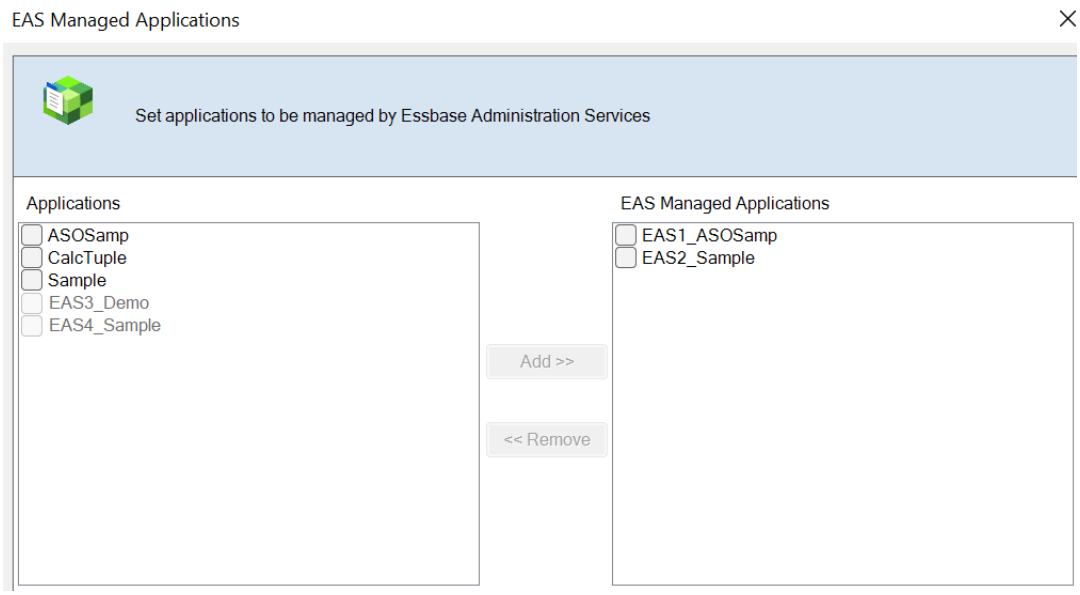
To manage applications using EAS Lite in cube designer,

1. In Excel, on the cube designer ribbon, select **Admin tasks**  .
2. Select **EAS Managed Applications**.




3. Enter your Essbase login credentials if prompted to do so.
4. In the **EAS Managed Applications** dialog box, select applications and use the **Add>>** and **<<Remove** options to switch to and from EAS Managed.

Once you have switched applications to EAS Managed and then switched them back to non-EAS Managed, those applications will be greyed out because you cannot go back to EAS Managed again.




**Caution:**

It's recommended to back up EAS managed applications before switching them back to being managed in the Essbase web interface, as this action is irreversible.

### Limitations of EAS Lite

Note the following limitations of EAS Lite:

- Global (server level) configuration settings are disabled.
- There are no EAS Console users in EAS Lite. Log in as an Essbase user, in whatever security model you're using.
- You can connect only to the Essbase server instance from which EAS Lite Console was launched, and you can't add other Essbase servers.
- You can't access Provider Servers.
- In the EAS Server node, **Edit properties** and **Externalize users** aren't available. In a particular EAS Server node, **Users** and **Properties** nodes aren't available.
- In the Essbase Servers node, **Add Essbase Server**, **Refresh Essbase Server List**, and **Show cluster information** aren't available.
- In the Connected Essbase Server node:
  - **View Log Charts** and **Generate logs** aren't available.
  - **Security** node and its child nodes **Users** and **Groups** aren't available.
- In the Cube node, **Preview data** isn't available.
- Essbase filter assignment within Shared Services isn't available.

- Under File > Wizards, **User Setup** and **Migration** aren't available.
- Within each application's action and context menus, **user/group access** and **Register** aren't available.
- Within each cube's action and context menus, **user/group access** isn't available.
- Outline conversion wizard (from block storage to aggregate storage) isn't available.
- When you are selecting aggregate views in Aggregation Design Wizard, charts are not displayed unless your JRE is bundled with JavaFX jars.

### Limitations of Essbase web interface for EAS-Managed Applications

When you're using an EAS-managed application, you can access it in the Essbase web interface as well as in EAS Lite, though some of the functionality in the Essbase web interface is unavailable. Examples of functionality not available for EAS-managed applications are:

- Outline editing (opens in view-only mode)
- Scenario management (new platform feature)
- Connections and datasources (new platform features)
- Drill through support (new platform features)

### Password is Required when Importing Partitions Exported to the File System

Starting in release 21.5, when a replicated or transparent partition is exported from EAS Lite to the file system as an XML file, password values of the source and target connections are not exported. When the exported partition XML file is imported back into EAS Lite, the password fields in the Partition dialog box in the EAS console are blank. During import, you must manually enter the password values in the source and target connections in the Partition dialog box.

### View Application and Agent Logs in EAS Lite

In Release 21.2.2.0.0 or higher, you can enable viewing the agent log from EAS Lite. You can also enable viewing trimmed logs for improved legibility in the Log Viewer.

### Application Logs in EAS Lite

By default, any user with Application Manager permission can view application logs.

To enable viewing trimmed application and agent logs, see the instructions below for setting ESSBASE_TRIM_ODL_LOGS to TRUE.

### Agent Log in EAS Lite

Only service administrators can view the agent log. As agent logs may contain system paths, they are not viewable by default in the Log Viewer. You must explicitly enable the ability to view agent logs in the Log Viewer, by setting an environment variable, ENABLE_ESSBASE_LOG_VIEW, to TRUE. If the environment variable is not set, EAS Lite returns a "permission denied" error.

### View Trimmed Logs in EAS Lite

By default, the Log Viewer displays log entries in Oracle Diagnostics Logging (ODL) format. The following is an example of an untrimmed ODL log entry:

```
[2021-11-03T16:31:52.180-07:00] [Sample] [NOTIFICATION:16] [MBR-120] [MBR]
[ecid: 1635982305564,0] [tid: 140444520277760] [REQ_ID: 61831be10000008c]
[DBNAME: Basic] Loading New Outline for Database [Basic] Succeeded
```

The following is an example of a trimmed log entry:

```
[2021-11-03T16:31:52.180-07:00][INFO][DBNAME: Basic]Loading New Outline for
Database [Basic] Succeeded
```

### Set the Log Display Options for EAS Lite

> **Caution:**
>
> The Essbase platform includes scripts in <*DOMAIN HOME*>/bin that can customize the environment and behaviors of Essbase functionality. However, making changes to these domain environment or startup scripts can have unintended effects, including startup failure. Oracle recommends making changes in a test environment first. Before editing these scripts, always:
>
> 1. Stop the Essbase managed servers, using <*DOMAIN HOME*>/esstools/bin/stop.sh (on Linux), or <*DOMAIN HOME*>\esstools\bin\stop.cmd(on Windows).
> 2. In <*DOMAIN HOME*>/bin, make a backup copy of the file you want to edit. For example,
>
>    On Linux
>
>    ```
>    cp setStartupEnv.sh setStartupEnv_bak.sh
>    ```
>
>    On Windows
>
>    ```
>    copy setStartupEnv.cmd setStartupEnv_bak.cmd
>    ```
>
> 3. Edit carefully, using only Oracle's documented instructions, or working with Oracle Support.
> 4. Restart Essbase, using <*DOMAIN HOME*>/esstools/bin/start.sh (on Linux), or <*DOMAIN HOME*>\esstools\bin\start.cmd(on Windows). Check that startup completed normally.

To enable viewing the agent log in the Log Viewer,

1. On the Essbase managed server machine, open one of the following startup files for editing. They are located in <DOMAIN HOME>/bin.
   - setEssbaseEnvOverrides.sh (or setEssbaseEnvOverrides.cmd)
   - setStartupEnv.sh (or setStartupEnv.cmd)
   - setDomainEnv.sh (or setDomainEnv.cmd)
2. Add a command to set the environment variable to enable Agent log to be viewed in Log Viewer by a service administrator.

   Linux example

   ```
   export ENABLE_ESSBASE_LOG_VIEW=TRUE
   ```

Windows example

```
set ENABLE_ESSBASE_LOG_VIEW=TRUE
```

3. Save the file and restart Essbase.

To enable trimmed log display in Log Viewer,

1. On the Essbase managed server machine, open `setDomainEnv.sh` for editing (or `setDomainEnv.cmd`, on Windows). It is located in <DOMAIN HOME>/bin.
2. Add a command to set the environment variable to view trimmed log format in Log Viewer.

   Linux example

   ```
   export ESSBASE_TRIM_ODL_LOGS=TRUE
   ```

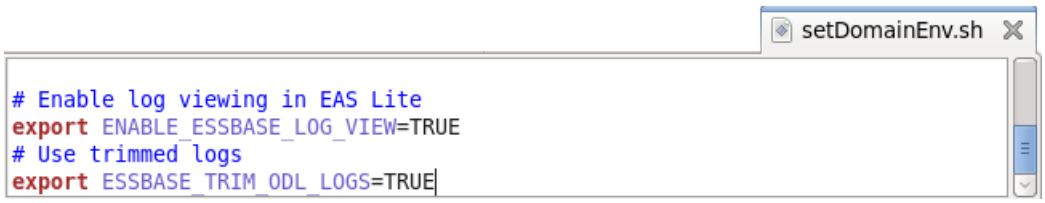
   Windows example

   ```
   set ESSBASE_TRIM_ODL_LOGS=TRUE
   ```

3. Save the file and restart Essbase.

**Sample Domain Environment Script**

The administrator has added these lines to the end of `setDomainEnv.sh`.



10

# Back Up and Restore Essbase

Essbase backup and restore planning is required at both the application and instance level to have full flexibility to manage the life cycle of your Essbase instances, and also to provide disaster recovery.

Backup and restore should be performed on the same version of Essbase, or at minimum between patchable versions of Essbase.

Essbase allows both Recovery Point Objective (RPO) and Recovery Time Objective (RTO) to be customized for your user base, supporting both instance-level and application-level backups. For example, if your RPO for most applications is twenty-four hours, then you must do an instance-level backup once a day. What if you have one application that needs to be backed up more often, say once every four hours? You can back up that application every four hours using LCM export. If you need to restore the instance, you can restore from the instance-level backup and then update that one application using the latest LCM export.

Backups of individual applications protect you from application failures or application artifact corruption, and can easily be migrated between servers. When you restore a single application, there is no disruption to user activity with other applications in your instance. Essbase application backups are taken using LCM export and import commands.

Essbase instance backups protect you against unplanned hardware or Essbase agent failures, which affect all applications on the instance. All user activity on the instance is affected for the duration of the recovery process, and all applications are restored to the point in time of the instance backup. Instance backups are also helpful when you are retiring older hardware.

You can use the backup and restore process in this chapter for your disaster recovery strategy and solution. See also Back Up and Restore Essbase: Weblogic Security Plus an Identity Provider , and Essbase on OCI Backup and Restore, a reference paper on disaster recovery and version upgrade planning, particularly for Essbase instances deployed on OCI.

Location aliases are migrated with the cube. LCM doesn't support Location alias credentials migration. After you migrate your applications from 11g you must replace your location aliases. See Location Aliases section in Prepare to Migrate From Essbase 11g.

## Scope of Back Up and Restore

Back up and restore discussed in this chapter is in the context of Essbase only. Oracle recommends that user and group management be external to your Essbase domain and on physically separate hardware to minimize disruptions during an Essbase restore event.

If you are using WebLogic security, configure your WebLogic domain with an identity provider installed on different hardware. This prevents your users and groups from being affected by any hardware failure where you run Essbase.

If you are using EPM Shared Services security with native Shared Services user and group management, install the EPM Foundation Services housing your Essbase users on separate hardware from where you have installed Essbase. Better still, use an identity provider with EPM Foundation Services.

> **Note:**
>
> WebLogic native user and group management is strongly discouraged and not supported for production instances. When using WebLogic security, always configure your WebLogic domain with an identity provider.

# Back Up and Restore Applications

Routine backup of Essbase applications ensures that you can recover from any sort of disruption to applications without affecting the other applications running on the same Essbase instance.

LCM export and import operations allow you to move applications on and off your Essbase instance or between Essbase instances. Export and import operations can be run sequentially in instance migration use cases, exporting from the source instance and importing into the target instance. However, to protect from unexpected application-level failures a routine backup cadence is required. The frequency of your application backups should correspond to the acceptable loss (recovery-point objective or RPO) specified by the application's users. At the time of any application-specific failure, the latest LCM export file can be used to recover all or part of the application.

> **Note:**
>
> Use LCM export option `--application` to export a single application to a zip file. Use option (case-sensitive) `--allApp` (or `-aa`), instead of `--application`, to export all applications to a single zip file. The `--allApp` option does not export users and groups.

By default, LCM export exports your application and its cubes without an itemized inventory of artifacts. When executing an LCM export, consider generating an artifact list. Only if you have included this artifact list on export will you have the option to selectively import specific components of your application and its cubes. To ensure backup consistency, make sure that the application is stopped before taking an LCM export.

> **Note:**
>
> For example, if using the CLI LcmExport command, you can use the optional `-generateartifactlist` parameter.

## Back Up Cube Files Using LCM

Use one of these tools to initiate an LCM Export operation, which backs up application and cube artifacts to a Lifecycle Management (LCM) .zip file:

- Command-line interface (CLI): LcmExport
- Essbase web interface Export LCM job
- REST API: Execute Job operation (using jobType **lcmexport**)

If you are migrating an application from an 11g version of Essbase, see Migrate an Essbase 11g On-Premises Application, and use the 11g Export Utility to take your backup. The backup commands discussed here are for exporting from later versions of Essbase.

## Restore Cube Files Using LCM

Use one of these tools to initiate an LCM Import operation, which restores application and cube artifacts from a Lifecycle Management (LCM) .zip file:

- Command-line interface (CLI): LcmImport
- Essbase web interface Import LCM job
- REST API: Execute Job operation (using jobType **lcmimport**)

> **Note:**
>
> After the LCM import completes, you may need to take further action to restore migrated connections to external sources. To do this, open the connection and enter the password.

# Back Up and Restore an Essbase Instance

Essbase instance backups are used to restore all applications on your instance to a common point in time. Instance backups are used primarily for disaster recovery, but are appropriate when you want to migrate or restore all applications at once.

Consider your pre-restore Essbase instance as a *source* (from which the backup is taken) and the post-restore Essbase instance as a *target*. After finishing the restore tasks, your applications in the target instance will reflect the source instance as of some point in time.

> **Note:**
>
> The target instance does not need to be the same version of Essbase as the source. However, the target version must be patchable compared to the source.

You will be told several times in these topics to stop your Essbase services. See Stop, Start, and Check Servers. After disabling user connections and before you stop the services, allow adequate time for existing user request to finish.

**Back Up an Essbase Instance**

Instance backups are a mandatory pre-requisite to restoring an Essbase instance, and you must examine backup consistency for Essbase 21c.

In addition to the disk artifacts used by Essbase 11g, Essbase 21c introduces the use of a relational database schema for managing Essbase application metadata. Modify your existing backup routines to ensure that you capture all relevant information in a consistent state.

To ensure that Essbase backups are consistent, stop all services before you take your backup. Although you can take steps to minimize this downtime, Oracle does not recommend taking instance backups while users are active. Before stopping Essbase, you may want to gracefully bring users off the system. See Alter Application (especially enable/disable) and Alter System

(especially logoff/ kill). If you use disable commands, you must reverse them with enable commands after you restart the system.

Consistent backups include:

- Contents of the <Application Directory>
- Relational database source schema: <schemaprefix>_Essbase
- EPM Shared Services “assigned roles” (if using EPM Shared Services with Essbase)

To minimize user downtime, consider mounting separate disk volumes for your `<Domain Root>/<Domain Name>` and your <Application Directory>. This will allow you to take snapshots or clones more quickly than compressing folders from the disk. Also, consider removing redundant or outdated text files used for loading data and building dimensions, as these can be quite large and will lengthen compression times.

**Restore an Essbase Instance**

Production Essbase instances use either WebLogic security plus an identity provider or EPM security (with or without an Identity Provider). In either case, users and groups are managed external to Essbase.

> **Note:**
>
> Embedded WebLogic LDAP is supported only for test environments and has significant backup and restore restrictions.

Generally speaking, your identity provider will not run on the same physical hardware as your Essbase instance, so you are protected from recovering the identity provider when you recover Essbase. You will only need to configure a new Essbase target instance and configure it to use your existing identity provider.

- Back Up and Restore Essbase: Weblogic Security Plus an Identity Provider
- Back Up and Restore Essbase: EPM Security Plus Shared Services Native Directory

# Back Up and Restore Essbase: Weblogic Security Plus an Identity Provider

Use the following process to back up and restore an Essbase instance if you are using WebLogic Security plus an identity provider.

## Back Up Essbase: WebLogic Security Plus an Identity Provider

Use the following process to back up an Essbase instance if you are using WebLogic Security plus an identity provider.

1. Back Up Contents of the Source Application Directory

   Your backup strategy for the source <*Application Directory*> will depend on the hardware used to create it. If you mounted a separate disk volume, then you have a portable backup. You should still routinely take a backup your <*Application Directory*> with every planned periodic backup.

   If you do not know where <*Application Directory*> is, see Environment Locations in the Essbase Platform.

If you haven't mounted your source <*Application Directory*> as a separate drive, you can simply compress its contents and safely move the archive to a secure, separate location. If you mounted a separate disk volume, you can copy the disk volume.

a. Check that the Essbase services are stopped. See Stop, Start, and Check Servers.

b. Navigate to the <*Application Directory*>.

   Example:

   ```
   cd /scratch/user/oracle_home/user_projects/applications/essbase
   ```

c. Compress the directory contents, providing the location and file name.

   There is no need to back up `jagentId.id`. A new one is created on the target, and you should not overwrite it. The example shows how to exclude it from the backup.

   ```
   tar -czvf <path to backup file location>/<backupfilename>.tar.gz --
   exclude jagentId.id *
   ```

   Example:

   ```
   tar -czvf /scratch/user/backups/appdir_backup.tar.gz --exclude
   jagentId.id *
   ```

2. Back Up the source Essbase Relational Database Schema.

Depending on the relational database you configured for use with Essbase, your steps may vary. The following example illustrates the use of Oracle Data Pump against supported Oracle Databases.

Execute Oracle Data Pump from the command line on the server where your Oracle Database is installed.

> **Note:**
>
> Alternatively, you can manage your database remotely using Oracle Instant Client.

Assume your source Essbase instance is deployed with a relational database schema prefix called `essbase1`.

a. Make sure that the source Essbase services are still stopped.

b. Confirm that the pluggable database (PDB) into which you deployed the Essbase schemas is in the `tnsnames.ora` file.

c. On the server running Oracle Database, create a directory path into which Data Pump can write database export files. Make sure the operating system user executing Data Pump commands has write privileges on this path.

   Example:

   ```
   mkdir /scratch/user/expuserfiles
   ```

d. Connect to the database containing the source Essbase schema.

e. Log in to SQL*Plus as sysdba, and create a role for your Data Pump user with the following minimum roles/privileges:

```
alter session set container=<your container name>;
create user <username> identified by <password>;
create directory <dirname> as '<full path disk location>';
create role <rolename>;
grant create session, create table to dp_role;
grant read, write on directory exports to <rolename>;
grant DATAPUMP_EXP_FULL_DATABASE to <rolename>;
grant DATAPUMP_IMP_FULL_DATABASE to <rolename>;
grant <rolename> to <username>;
alter user <username> default tablespace users;
alter user <username> quota unlimited on users;
exit;
```

Example:

```
alter session set container=orclpdb;
create user expuser identified by password;
create directory exports as '/scratch/user/expuserfiles';
create role dp_role;
grant create session, create table to dp_role;
grant read, write on directory exports to dp_role;
grant DATAPUMP_EXP_FULL_DATABASE to dp_role;
grant DATAPUMP_IMP_FULL_DATABASE to dp_role;
grant dp_role to expuser;
alter user expuser default tablespace users;
alter user expuser quota unlimited on users;
exit;
```

f. Execute Oracle Data Pump from the command line on the server where Oracle Database is installed.

> **Note:**
>
> Alternatively, you can manage your database remotely using Oracle Instant Client.

On the server where Oracle Database is running, export the <*schemaprefix*>_Essbase schema using the Data Pump `expdp` command:

> **Note:**
>
> Be sure to set the Oracle environment for your database before running Data Pump.

```
expdp <username>@<service name> directory=<dirname>
dumpfile=<dumpfilename>.dmp logfile=<logname>.log
schemas=<schemaprefix>_Essbase
```

Example:

```
expdp expuser@orclpdb directory=exports dumpfile=essbase1.dmp
logfile=essbase1.log schemas=essbase1_Essbase
```

## Restore Essbase: WebLogic Security Plus an Identity Provider

Use the following process to restore an Essbase instance if you are using WebLogic Security plus an identity provider.

1. Configure a target Essbase instance.

   If your source host/hardware didn't fail and you are just recovering your Essbase instance, you can unconfigure the source instance and then configure a new target instance using the same Fusion Middleware <*ORACLE_HOME*>.

   If you do not know where <*ORACLE_HOME*> is, see Environment Locations in the Essbase Platform.

   a. Use the Essbase Configuration Tool to configure a target Essbase instance. The configuration tool is located at:

      ```
      /<path to Fusion Middleware Oracle Home>/essbase/bin/config.sh
      ```

      Example:

      ```
      /scratch/user/oracle_home/essbase/bin/config.sh
      ```

   b. Configure the target domain:

      i. Use the same WebLogic administrator username and password as is used in the Essbase source instance.

      ii. Use the same domain name as is used in the source instance.

      iii. Use the same <*Application Directory*> as is used in the source instance.

      It is essential that the full <*Application Directory*> is identical on the target instance, otherwise, some Essbase functionality will not work.

      If you do not know where <*Application Directory*> is, see Environment Locations in the Essbase Platform.

      iv. You may use the same pluggable database (PDB), or a different one.

      > **Note:**
      >
      > You will need a new schema prefix, unless you removed your source schemas during unconfiguration.

      v. Do not select EPM Shared Services security.

   Refer to your configuration response file from the source instance, which was originally created at `/tmp/essbase_config_<date_timestamp>/config.rsp`.

2. Configure an identity provider.

   After configuring your target instance, configure your identity provider. See WebLogic Authentication.

> **Note:**
>
> When you configured your source domain, you may have selected a federated user and assigned system administrator role to that user. In that case, you do not need to assign roles in this new target domain.

3. Restore the <*Application Directory*> contents from the source backup into the target instance.
   a. Confirm that all services on the target instance are stopped. See Stop, Start, and Check Servers.
   b. Move the existing/source <*Application Directory*> to a different location.

      Example:

      ```
      mv /scratch/user/oracle_home/user_projects/applications/essbase /
      scratch/user/oracle_home/user_projects/applications/essbase.old
      ```

   c. Create the new/target <*Application Directory*>.

      Example:

      ```
      mkdir /scratch/user/oracle_home/user_projects/applications/essbase
      ```

   d. Navigate to the new/target <*Application Directory*>.

      Example:

      ```
      cd /scratch/user/oracle_home/user_projects/applications/essbase
      ```

   e. Unzip the contents of the source <*Application Directory*> backup into the new/target <*Application Directory*> (directories extracted may include `app`, `catalog`, and `hybrid`, depending on what you backed up).

      ```
      tar -zxvf <path to backup file location>/<backup file name>.tar.gz
      ```

      Example:

      ```
      tar -zxvf /scratch/user/backups/appdir_backup.tar.gz
      ```

4. Restore the Essbase Relational Database Schema.

   Depending on the relational database you configured for use with Essbase, your steps may vary. The following example illustrates the use of Oracle Data Pump against supported Oracle Databases.
   a. Confirm that all services on the target instance are stopped.
   b. Execute Oracle Data Pump from the command line on the server where Oracle Database is installed.

      > **Note:**
      >
      > Alternatively, you can manage the database using Oracle Instant Client.

c. Import the Essbase source schema backup (.dmp file) into the target, replacing the source schema prefix with the target schema prefix:

```
impdp <username>@<service name> directory=<dirname> dumpfile=<source
dumpfilename>.dmp REMAP_SCHEMA=<source schemaprefix>_Essbase:<target
schemaprefix>_Essbase partition_options=merge
table_exists_action=replace
```

Example:

```
impdp expuser@orclpdb directory=exports dumpfile=essbase1.dmp
REMAP_SCHEMA=essbase1_ESSBASE:essbase2_ESSBASE partition_options=merge
table_exists_action=replace
```

5. Start target instance Essbase services. See Stop, Start, and Check Servers.

# Back Up and Restore Essbase: EPM Security Plus Shared Services Native Directory

Use the following process to back up and restore an Essbase instance if using EPM Security Plus Shared Services Native Directory.

## Back Up Essbase: EPM Security Plus Shared Services Native Directory

Use the following process to back up an Essbase instance if using EPM Security Plus Shared Services Native Directory.

1. Back Up Contents of the Source Application Directory
   Your backup strategy for the <Application Directory> will depend on the hardware used to create it. If you mounted a separate disk volume, then you have a portable backup. You should still routinely take a backup your <Application Directory> with every planned periodic backup.

   If you haven't mounted your <Application Directory> as a separate drive, you can simply compress its contents and safely move the archive to a secure, separate location. If you mounted a separate disk volume, you can copy the disk volume.

   a. Check that your Essbase services are stopped. See Stop, Start, and Check Servers.

   b. Go to the <Application Directory>.

   ```
   cd <Application Directory>
   ```

   Example:

   ```
   cd /scratch/user/oracle_home/user_projects/applications/essbase
   ```

   c. Compress the directory contents, providing the location and file name.

   ```
   tar -czvf <path to backup file location>/<backupfilename>.tar.gz *
   ```

Example:

```
tar -czvf /scratch/user/expuserfiles/appdir_backup.tar.gz *
```

2. Back Up the source Essbase Relational Database Schema.
Depending on the relational database you configured for use with Essbase, your steps may vary. The following example illustrates the use of Oracle Data Pump against supported Oracle Databases.

   Execute Oracle Data Pump from the command line on the server where your Oracle Database is installed.

   > **Note:**
   >
   > Alternatively, you can manage your database remotely using Oracle Instant Client.

   Assume your source Essbase instance is deployed with a relational database schema prefix called "essbase1."

   a. Make sure that your source Essbase services are still stopped.

   b. Confirm that the pluggable database (PDB) into which you deployed your Essbase schemas is in your `tnsnames.ora` file.

   c. On the server running your Oracle Database, create a directory path into which Data Pump can write database export files. Make sure the operating system user executing datapump commands has write privileges on this path.
   Example:

   ```
   mkdir /scratch/user/expuserfiles
   ```

   d. Connect to the database containing your source Essbase schema.

   e. Log in to SQLplus as sysdba and create a role for your datapump user with the following minimum roles/privileges:

   ```
   alter session set container=<your container name>;
   create user <username> identified by <password>;
   create directory <dirname> as '<full path disk location>';
   create role <rolename>;
   grant create session, create table to dp_role;
   grant read, write on directory exports to <rolename>;
   grant DATAPUMP_EXP_FULL_DATABASE to <rolename>;
   grant DATAPUMP_IMP_FULL_DATABASE to <rolename>;
   grant <rolename> to <username>;
   alter user <username> default tablespace users;
   alter user <username> quota unlimited on users;
   exit;
   ```

   Example:

   ```
   alter session set container=orclpdb;
   create user expuser identified by password;
   create directory exports as '/scratch/user/expuserfiles';
   ```

```
create role dp_role;
grant create session, create table to dp_role;
grant read, write on directory exports to dp_role;
grant DATAPUMP_EXP_FULL_DATABASE to dp_role;
grant DATAPUMP_IMP_FULL_DATABASE to dp_role;
grant dp_role to expuser;
alter user expuser default tablespace users;
alter user expuser quota unlimited on users;
exit;
```

f. Execute Oracle Data Pump from the command line on the server where your Oracle Database is installed.

> **Note:**
>
> Alternatively, you can manage your database remotely using Oracle Instant Client.

On the server where your database is running, export the <*schemaprefix*>_Essbase schema using the Data Pump `expdp` command:

> **Note:**
>
> Be sure to set the Oracle environment for your database before running Data Pump.

```
expdp <username>@<service name> directory=<dirname>
dumpfile=<dumpfilename>.dmp logfile=<logname>.log
schemas=<schemaprefix>_Essbase
```

Example:

```
expdp expuser@orclpdb directory=exports dumpfile=essbase1.dmp
logfile=essbase1.log schemas=essbase1_Essbase
```

3. Back up EPM Shared Services assigned roles.
This step does not apply to WebLogic security. In the case of EPM Shared Services security, Essbase application permissions aren't stored or managed in Essbase. Rather, Essbase user and application roles are assigned to users and groups using EPM Shared Services.

   EPM Shared Services stores these roles, so it is important to take backups using the Shared Services Console that contain your Essbase users and groups.

> **Note:**
>
> These backup instructions apply to the Shared Services Console that houses users and groups for Essbase, and not the main EPM Shared Services that contains all the Planning and other EPM applications users and groups.

a. In EPM Shared Services, expand **Foundation** in the **Application Groups** section.

b. Select **Shared Services**.

c. Select **Native Directory**.

d. Click **Export** (bottom right).
Exported files are moved into the `<EPM_Instance>/import_export` folder by default.

## Restore Essbase: EPM Security Plus Shared Services Native Directory

Follow these steps to restore Essbase using EPM Shared Services security plus Shared Services Native Directory.

1. Configure a target Essbase instance.
If your source host/hardware didn't fail and you are just recovering your Essbase instance, you can unconfigure the source instance and then configure a new target instance using the same Fusion Middleware <Oracle Home>.

   a. Use the Essbase Configuration Tool to configure a target Essbase instance.

   ```
   /<path to Fusion Middleware Oracle Home>/essbase/bin/config.sh
   ```

   Example:

   ```
   /scratch/user/oracle_home/essbase/bin/config.sh
   ```

   b. Configure the target domain:

      i. Use the same WebLogic admin username and password as the Essbase source instance.

      ii. Use the same domain name as the source.

      iii. Use the same <Application Directory> as the source.

      > **Note:**
      >
      > It is essential that the full application directory is idential for target instance, otherwise, some Essbase functionality will not work.

      iv. You may use the same pluggable database (PDB), or a different one.

      > **Note:**
      >
      > You will need a new schema prefix, unless you removed your source schemas during unconfigure.

      v. Select EPM security and use the same EPM_ORACLE_HOME and EPM_ORACLE_INSTANCE.

   Refer to your configuration response file from the source instance, which was originally created at `/tmp/essbase_config_<date_timestamp>/config.rsp`.

2. Restore the <Application Directory> Folder Contents from the Source Backup into the Target Instance.

a. Confirm that all services on the target instance are stopped. See Stop, Start, and Check Servers.

b. Move the existing <Application Directory> to a different location.

```
mv <Application Directory> <Application Directory>.old
```

Example:

```
mv /scratch/user/oracle_home/user_projects/applications/essbase /
scratch/user/oracle_home/user_projects/applications/essbase.old
```

c. Create the <Application Directory>.

```
mkdir /<Application Directory>
```

Example:

```
mkdir /scratch/user/oracle_home/user_projects/applications/essbase
```

d. Go to the <Application Directory>.

```
cd <Application Directory>
```

Example:

```
cd /scratch/user/oracle_home/user_projects/applications/essbase
```

e. Unzip the contents of the source <Application Directory> backup into the target <Application Directory> (app, catalog, hybrid, jagentID.id).

```
tar -zxvf <path to backup file location>/<backup file name>.tar.gz
```

Example:

```
tar -zxvf /scratch/user/expuserfiles/appdir_backup.tar.gz
```

3. Restore the Essbase Relational Database Schema.
Depending on the relational database you configured for use with Essbase, your steps may vary. The following example illustrates the use of Oracle Data Pump against supported Oracle Databases.

a. Confirm that all services on the target instance are stopped.

b. Execute Oracle Data Pump from the command line on the server where your Oracle Database is installed.

> **Note:**
>
> Alternatively, you can manage your database using Oracle Instant Client.

c. Import the Essbase source schema backup (.dmp file) into the target, replacing the source schema prefix with the target schema prefix:

```
impdp <username>@<service name> directory=<dirname> dumpfile=<source
dumpfilename>.dmp REMAP_SCHEMA=<source schemaprefix>_Essbase:<target
schemaprefix>_Essbase partition_options=merge
table_exists_action=replace
```

Example:

```
impdp expuser@orclpdb directory=exports dumpfile=essbase1.dmp
REMAP_SCHEMA=essbase1_ESSBASE:essbase2_ESSBASE partition_options=merge
table_exists_action=replace
```

4. Import Source Assigned Roles Into Shared Services.

> **Note:**
>
> Shared Services is not stopped during this process.

Because this is EPM security, roles are not managed natively in Essbase. Instead, they are managed in Shared Services, so import source Assigned Roles into Shared Services, which is now registered with the target Essbase domain.

a. In Shared Services, under **File System**, expand your <Shared Services> backup and select HSS-<Shared Services *BackupName*>.

b. Expand **Native Directory**.

c. Expand **Assigned Roles**.

d. Select **EssbaseCluster-1** to restore all Essbase application and server access roles in your target Essbase instance.

e. Click **Import** (bottom right), and click **OK**.

5. Start the target instance.
Start target instance Essbase services. See Stop, Start, and Check Servers.

# Advanced Backup and Restore Tasks

These sections describe some advanced Essbase instance backup and restore tasks.

**Server Configuration Files**

If you have made any customizations to `essbase.cfg` or `odbc.ini` files, you should back them up each time you back up the instance.

**Network Security Certificates**

Certificate updates that you applied on your source instance must also be applied on your recovered target instance for all of the same Essbase functionality to work.

**Partitions Across Hosts**

If your instance contains partitioned Essbase applications and your recovered target instance is on a different host (ie target has different IP or a different fully qualified hostname), you will need to delete and re-create your partitions after recovery onto the target machine.

Alternatively, you can add the qualified hostname from your source instance to the `/etc/hosts` file on your target instance.

Deleting partitions can be done on the file system by deleting `.ddb` files from both partition source and partition target database folders

# Change Relational Database Server or Port

As part of the Backup/Restore process, you can reconfigure Essbase using a new Oracle database instance. This topic show how to change your relational database server or port.

**Change Relational Database Server**

1. Stop the current running Essbase instance.

```
cd <Oracle_HOME>/user_projects/domains/essbase_domain/esstools/bin
./stop.sh
```

2. Create a new database `<export_user_name>` user and run 'expdp' command to make a schema backup. Only export the RCUPrefix_essbase schema.
For example:

```
alter session set container="containername";
create user <export_user_name> identified by <password>;
grant create session, create table to <export_user_name>;
create or replace directory dmpdir to <export_user_name>;
grant DATAPUMP_EXP_FULL_DATABASE to <export_user_name>;
grant DATAPUMP_IMP_FULL_DATABASE to <export_user_name>;
grant user <export_user_name> default tablespace users;
alter user <export_user_name> quota unlimited on users;
exit;
```

```
expdp <export_user_name>/<password>@<pdbname> dumpfile=<RCUPrefix>.dmp
logfile=<RCUPrefix>.log schema=<RCUPrefix>_ESSBASE directory=dmpdir
```

3. It is **highly** recommended to make a backup of your applications directory. If you already have a backup, or your applications directory has many large applications, you can skip this step.
For example:

```
cd user_projects/applications/essbase/
tar -cvfz ~/Backup/Apps.tar.gz app/*
```

4. Configure a new Essbase instance against a new Oracle database. You will have a chance to enter the Domain Root and Application Directory path - with the following options:
    - If you want to re-use 'user_projects' as the main instance, and since it's already being used by the old instance, then rename the old user_projects to something else before launching Configuration Tool.
    - Or enter a new 'user_projects_XXX' for Domain Root and Application Directory path of a new configuration.

> **Note:**
>
> Do not try to remove anything until a new instance is up and running.

For example, (on the **Domain Details** configuration page, where you select Domain and Application locations):

- **Domain Name** `essbase_domain`
- **Domain Root** `Oracle/21.4.2/Middleware/Oracle_Home/user_projects/domains`
- **Application Directory** `/Middleware/Oracle_Home/user_projects/applications/essbase`
- **WebLogic Administrator Account**
  ...

5. Finish configuring a new Essbase instance against a new Oracle database. Make sure to use a new schema name.
6. Stop Essbase again (see step #1) after Configure Tool is done.
7. Create a similar ‘expuser’ user for the new Oracle database and run ‘impdp’ command to restore data from dumpfile obtained from backup in step #3. Import RCUPrefix_essbase schema only with the remap option, if the new schema has a new name.
   For example:

```
alter session set container="containername";
create user <export_user_name> identified by <password>;
grant create session , create table to <export_user_name>;
create or replace directory dmpdir to <export_user_name>;
grant DATAPUMP_EXP_FULL_DATABASE to <export_user_name>;
grant DATAPUMP_IMP_FULL_DATABASE to <export_user_name>;
grant user <export_user_name> default tablespace users;
alter user <export_user_name> quota unlimited on users;
exit;
```

```
impdp expuser/<password>@<pdbname>  dumpfile=<schema_name>.dmp
logfile=<schema_name>.log REMAP_SCHEMA=[OLD_SCHEMA]_ESSBASE:
[NEW_SCHEMA]_ESSBASE directory=dmpdir partition_options=merge
table_exists_action=replace
```

8. Restore applications directory from the backup or move it from the previous instance.

```
cd user_projects/applications/essbase/
tar xvf ~/Backup/Apps.tar
```

9. Start Essbase for the new instance and make sure everything is running successfully. Since you haven’t deleted anything, you can always go back to the previous good instance if necessary. Once everything is working, then you can go ahead and clean up what you don’t need.

```
cd <Oracle_HOME>/user_projects/domains/essbase_domain/esstools/bin
./start.sh
```

10. Note that all of the settings of the old managed servers in WebLogic, once new configuration is done, need to be manually added to the newly created managed servers.

**Change Database Server Port Only**

1. Stop Essbase server.

```
cd <Oracle_HOME>/user_projects/domains/essbase_domain/esstools/bin./stop.sh
```

2. Change the database port in tnsnames.ora and listener.ora files, on the database server, to your required port, for example, 1524.
3. Restart listener and restart the database. Check the connection in sql developer.
4. In the following location on the Essbase server, do the following:

```
cd <ORACLE_HOME>/user_projects/domains/essbase_domain/config/fmwconfig
```

In jps-config.xml, change the port to the new port in this property.

```
<property name="jdbc.url"
value="jdbc:oracle:thin:@(description=(address=(host=DBhost)(protocol=tcp)
(port=1524))(connect_data=(service_name=DBPDBname)(server=dedicated)))"/>
```

In jps-config-jse.xml, make a similar change to the properties that refer to the database port.

```
<property name="jdbc.url"
value="jdbc:oracle:thin:@(description=(address=(host=DBhost)(protocol=tcp)
(port=1524))(connect_data=(service_name=DBPDBname)(server=dedicated)))"/>
```

5. In the following location, do the following:

```
cd <ORACLE_HOME>/user_projects/domains/essbase_domain/config/jdbc
```

Change the database port to the new port number in the following files
essbase_datasource-jdbc.xml

```
<url>jdbc:oracle:thin:@(description=(address=(host=DBHost)(protocol=tcp)
(port=1524))(connect_data=(service_name=DBPDBName)(server=dedicated)))</
url>
```

LocalSvcTblDataSource-jdbc.xml

```
<url>jdbc:oracle:thin:@(description=(address=(host=DBHost)(protocol=tcp)
(port=1524))(connect_data=(service_name=DBPDBName)(server=dedicated)))</
url>
```

opss-audit-jdbc.xml

```
<url>jdbc:oracle:thin:@(description=(address=(host=DBHost)(protocol=tcp)
(port=1524))(connect_data=(service_name=DBPDBName)(server=dedicated)))</
url>
```

opss-auditview-jdbc.xml

```
 <url>jdbc:oracle:thin:@(description=(address=(host=DBHost)(protocol=tcp)
(port=1524))(connect_data=(service_name=DBPDBName)(server=dedicated)))</
url>
```

opss-datasource-jdbc.xml

```
<url>jdbc:oracle:thin:@(description=(address=(host=DBHost)(protocol=tcp)
(port=1524))(connect_data=(service_name=DBPDBName)(server=dedicated)))</
url>
```

WLSSchemaDataSource-jdbc.xml

```
 <url>jdbc:oracle:thin:@(description=(address=(host=DBHost)(protocol=tcp)
(port=1524))(connect_data=(service_name=DBPDBName)(server=dedicated)))</
url>
```

6. In the following location, do the following:

```
cd <ORACLE_HOME>/user_projects/domains/essbase_domain/init-info
```

Change the database port, in the following files, to the new port number.
startup-plan-unsub.xml:

```
 <jvm:value>'OCI;SERVICE=DBHost:1524/DBPDBName'</jvm:value>
```

startup-plan.xml:

```
<jvm:value>'OCI;SERVICE=DBHost:1524/DBPDBName'</jvm:value>
```

7. Restart Essbase.

```
cd <Oracle_HOME>/user_projects/domains/essbase_domain/esstools/bin
./start.sh
```

11

# Troubleshooting

This section provides information to assist you in addressing errors and issues with Essbase deployment.

Check log files to diagnose problems. For log file locations, see Environment Locations in the Essbase Platform.

If you cannot connect to Essbase services that are running, check whether your repository database schema passwords are expired. See Reset Essbase Repository Database Schema Passwords.

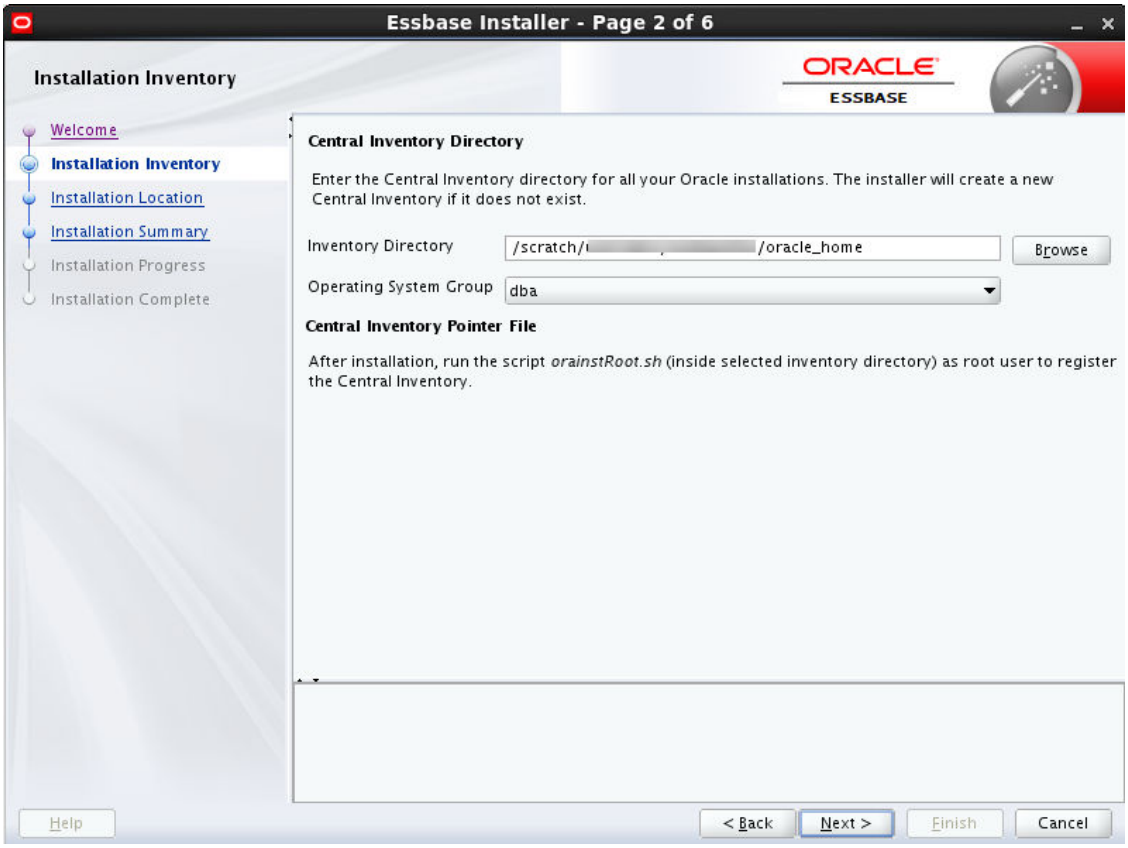
**Topics:**



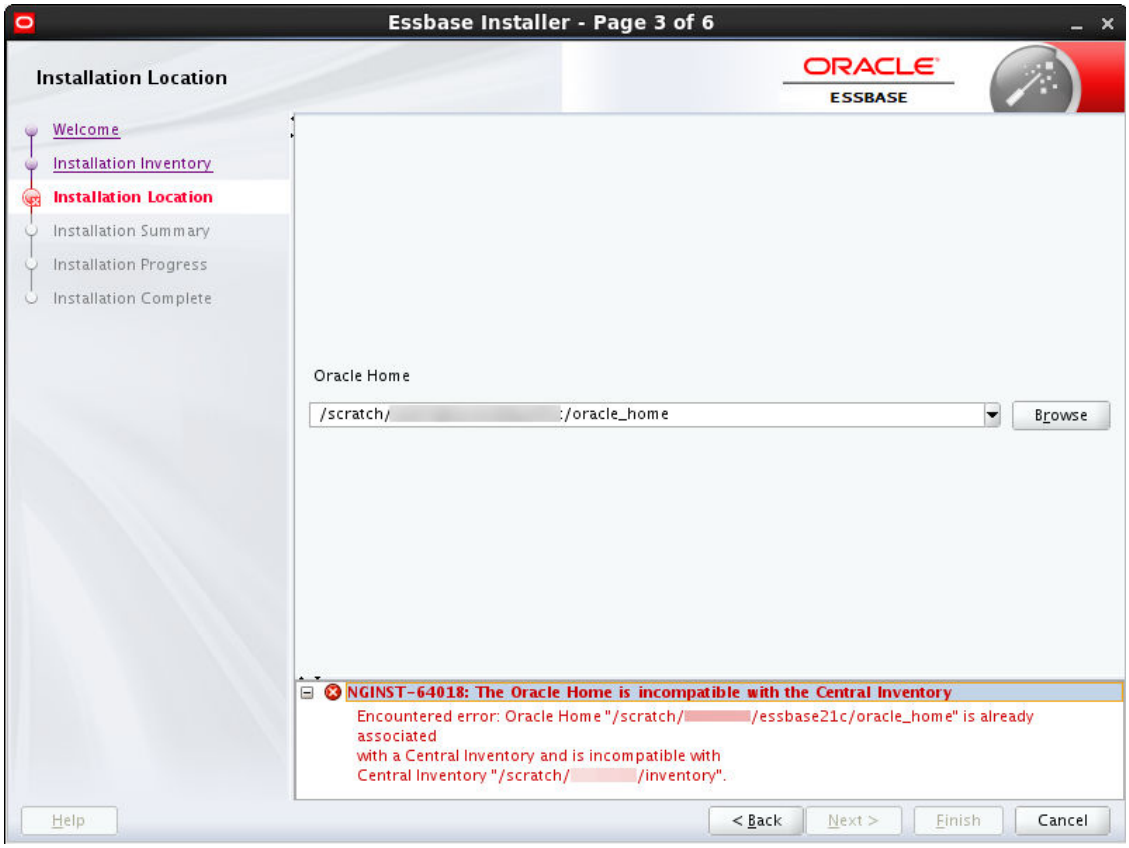
## Specify Inventory Location

The Essbase installer attempts to detect the inventory location for Fusion Middleware.

If the `oraInst.loc` for Fusion Middleware isn't detected, you're prompted to provide the central inventory location in the Installation Inventory screen.




Some Oracle products may set a central inventory location in `/etc`. If you have a central inventory location in `/etc`, you may encounter an error during the installation.




If you encounter experience this error, you can explicitly specify the Fusion Middleware inventory location using the `-invPtrLoc` argument to the installer.

For example, launch the installer as follows:

```
java -jar essbase-21.1.0.0.0-linux64.jar -invPtrLoc /scratch/username/
essbase21c/oracle_home/oraInst.loc
```

# Avoid Port Conflicts

Ensure that the ephemeral port range used by the operating system does not conflict with any reserved Essbase ports.

Also ensure that the range does not conflict with any ports occupied by other services, such as EPM Foundation Services, Oracle HTTP Server, or any other load balancer you may be using. In addition, no Essbase ports should be in use by other processes.

Essbase ports include:

- Node manager port
- WebLogic ports, including
  - AdminServer port
  - Essbase managed server ports, both clear and secure
  - Essbase Administration Services (EAS) managed server ports (if used), both clear and secure
- Essbase agent (JAgent) ports (clear and secure)

- Essbase application server (ESSSVR) ports (1000-port range)

Your operating system's ephemeral port range is a reserved set of temporary port allocations. Conflicts can arise if any assigned Essbase ports fall within the ephemeral port range.

To check your operating system's ephemeral port range, use the following command:

**For Linux:**

```
cat /proc/sys/net/ipv4/ip_local_port_range
```

**For Windows:**The following will list the ports occupied (listening) in Windows:

```
netstat -a -b
```

# GCC-C++ Not Found after Essbase Installation

The c++ compiler, gcc-c++ is a prerequisite for installation. If you receive an error regarding gcc-c++ as missing or not installed compiler, use this workaround.

1. Run the install command:

   ```
   yum install gcc-c++
   ```

   as root user.
2. Run the generate command. ORACLE_HOME must be defined prior to running this command.

   ```
   $ORACLE_HOME/bin/genoccish
   ```

# EAS Lite Troubleshooting

Refer to these tips if you need to troubleshoot the Essbase Administration Services (EAS) Lite web console.

### EAS Lite Web Console Stops Responding During User Provisioning

If you use the web console version of Essbase Administration Services (EAS) Lite, and your authentication provider is EPM Shared Services, the web console may stop responding while you are trying to provision users.

Solution: Open EPM Shared Services using one of the older, supported web browsers listed in Oracle Hyperion EPM 11.1.2 Certification Matrix. For example, Firefox 68.2.0 ESR(32-bit).

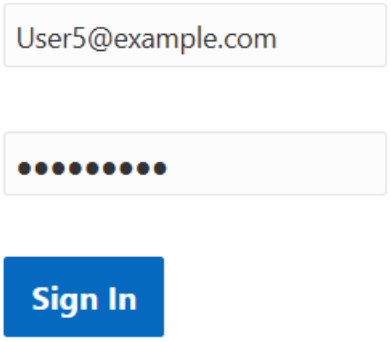
# MSAD Federated Log In

In the Essbase web interface, you may need to provide the domain suffix when you log in to Essbase as a federated Microsoft Active Directory (MSAD) user. When logging in using MaxL, you don't need the domain suffix.

**MaxL Example**

```
login user User5 P855w0r$4 on "https://192.0.2.1:9001/essbase/agent";
```

**Web Interface Example**




# Network Error Upon Create or Import Application

To create or import applications on independent deployments on Linux, Essbase requires system access to `/tmp/app`.

The following network error may occur when creating or importing an application:

```
"Network error []: Failed to connect to [appname]
```

If you experience this error on a Linux installation of Essbase, ensure that you have permission to the `/tmp/app` directory.