CA Executive Insight for Service Assurance Administration and Configuration Guide

Release 2.0

CA Technologies Product References

This document references the following CA Technologies products and features:

- CA Executive Insight for Service Assurance
- CA Application Performance Management (CA APM)
- CA Customer Experience Manager (CA CEM)
- CA Embedded Entitlements Manager (CA EEM)
- CA Introscope®
- CA SiteMinder®
- CA Capacity Command Center (CA CCC)
- CA Service Operations Insight (CA SOI)
- CA APM Cloud Monitor

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Overview

This guide is for Administrators and describes how to install and configure CA Executive Insight.

Chapter 2: Deployment Options

The CA Executive Insight installer supports the following deployment solutions. To prepare for your deployment, review the options.

Intranet Only

- Recommended for sites with existing secure ways for users to access the internal corporate network from their mobile devices, using VPN or Mobile Data Management (MDM) options.
- During installation, select the component, "Server and Mobile Application User Interface."
- If you are upgrading from a previous version of the product, the intranet only option is installed by default.

Internet Accessible

- Recommended for sites that want users to access CA Executive Insight directly from the Internet without being logged in to the internal corporate network.
- During installation:
  - Select the component, "Server and Mobile Application User Interface" and install it on a server behind firewalls.
  - Additionally, install the "Mobile Application User Interface" component on a server in the DMZ.
    - Deploy this component on a different machine from the Server and Mobile Application User Interface.
    - This component communicates with the "Server and Mobile Application User Interface" on its HTTP/HTTPS port. The HTTP/HTTPS port is the only port that must be opened on the firewall between the two machines. Also, this port must have direct access to the internet, or use a reverse proxy.
- The Admin UI can be accessed only from the intranet on the “Server and Mobile Application User Interface” component.

Chapter 3: Install CA Executive Insight on Windows

Install CA Executive Insight on Windows

CA Executive Insight supports *business indicators* that are mapped to IT metrics. You create business indicators that are based on the available metrics from different data sources in your environment.

A *metric connector* creates a connection between a data source and the CA Executive Insight application. After the connection is established, the application retrieves IT metrics from the data source and publishes the metric data as business indicators in a dashboard.

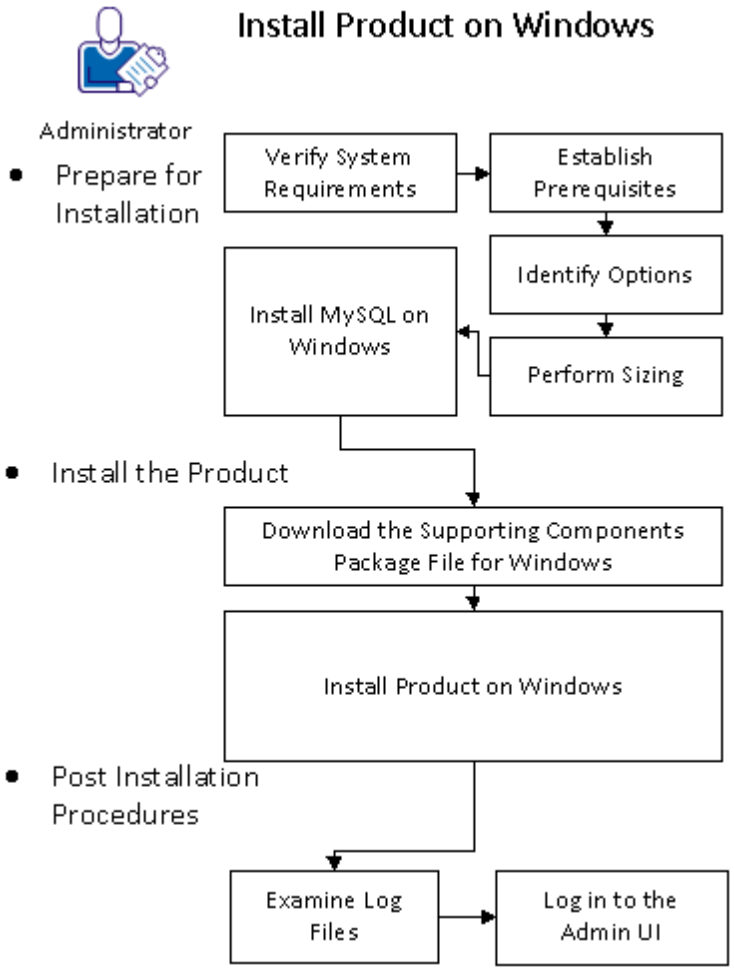
Many data sources are supported:

- CA Application Performance Management (CA APM)
- CA Service Operations Insight (CA SOI)
- CA Capacity Command Center (CA CCC)
- Comma-separated values files (CSV files)
- Web services connectors

To retrieve data, add a connector and specify the connection information for the instance.

Before you configure metric connectors and build business indicators for your mobile device users, complete the installation of CA Executive Insight.

The following illustration describes how an administrator installs CA Executive Insight on a Windows host.



To complete the installation of CA Executive Insight on Windows, follow these steps:

1. Prepare for installation:
   a. Verify system requirements (see page 13)
   b. Establish prerequisites (see page 15)
   c. Identify options (see page 15)
   d. Perform sizing (see page 18)
   e. Install MySQL on Windows (see page 21)

2. Install the product:
   a. Download the supporting components package file for Windows (see page 25)
   b. Install CA Executive Insight on Windows (see page 25)
3. Post-installation procedures:
   a. Examine log files (see page 28)
   b. Log in to the Admin UI (see page 28)

Verify System Requirements

Verify that the following system requirements are filled before you install CA Executive Insight:

Server Requirements

The following platforms are supported:

- Windows 2008 64-bit
- Linux Red Hat 5 and Red Hat 6 64-bit

Data Source Requirements

The following CA Technologies product versions are supported:

- CA APM 9.0.x and 9.1.x

  CA Executive Insight can retrieve CA Introscope® metrics from an Enterprise Manager in a standalone environment or a Manager of Managers (MOM) Enterprise Manager in a clustered environment. If the APM instance is connected to Transaction Impact Monitors (TIMs), Customer Experience metrics also are available.

- CA Introscope® 8.1.1, 8.2, 9.0.x and 9.1.x

  CA Executive Insight can retrieve CA Introscope® metrics from an Enterprise Manager in a standalone environment or a MOM Enterprise Manager in a clustered environment.

- CA CEM 4.5

  CA Executive Insight can retrieve customer experience metrics from a Customer Experience Manager instance.

- CA Service Operations Insight 3.0

  CA Executive Insight can retrieve the business service hierarchy and service metrics from CA SOI.

- CA Capacity Command Center 2.1.0

  CA Executive Insight can retrieve the group hierarchy from CA Capacity Command Center and the corresponding efficiency metrics.

Mobile Requirements

CA Executive Insight is a web application that is designed to run on any mobile platform with a browser that supports WebKit. The supported browsers include Safari, Google Chrome, or Android.

CA Executive Insight is certified on the following mobile devices:

- Android 7 and 10-inch tablets running Android OS 4.x, such as Google Nexus 7 running Android 4.1 and Samsung Galaxy Tab 2 running Android 4.0 with the Chrome browser.
- Apple iPhone 4, iPhone 4S, and iPhone5 running the Safari browser with iOS 6.1.
- Apple iPad 2, iPad 3, and iPad 4 running the Safari browser with iOS 6.1.

  Note: CA Executive Insight 2.0 and 1.3 do not support iPad 1.
- Smartphones running Android 2.3 such as HTC Incredible 2 running the default Android browser that is shipped with the OS.
- Smartphones running Android 4.x, such as Samsung S2 or Samsung S3, Samsung Galaxy Nexus, with the Chrome browser.

  Note: CA Executive Insight 1.3 and 2.0 do not support Blackberry Playbook.

CA Executive Insight supports administrators running the mobile user interface on the following desktop browsers:

- Safari 5.1.x
- Google Chrome 25.x

  Note: The preceding platforms have been certified at the time of General Availability (GA). Given rapidly changing technology, for current information regarding platform support, see the CA Executive Insight Support web page at http://ca.com/support.

Admin UI Browser Requirements

To administer CA Executive Insight, log in to the Admin UI using a browser.

The Admin UI is certified on the following browsers:

- Internet Explorer 8 and 9
- Firefox 19.x

Note: The preceding browsers have been certified at the time of General Availability (GA). Given rapidly changing technology, for current information regarding browser support, see the CA Executive Insight Support web page at http://ca.com/support.

Supported Security Standards

CA Executive Insight complies with the FIPS 140-2 standard.

Establish Prerequisites

Before you install the product, review the following requirements:

- MySQL Enterprise Edition 5.5.8

  The product stores its data in a MySQL database. The required MySQL packages are provided with the product, install them separately. You do not need to reinstall MySQL when upgrading from an older version of the product.

- CA Embedded Entitlements Manager (CA EEM) 8.4 or 12.0

  CA EEM is used to authenticate and authorize the users that log in to CA Executive Insight. Before you can log in to CA Executive Insight, set up a user in CA EEM. To set up a user, create a user in the CA EEM local store. Alternatively, you can configure CA EEM to connect to your Active Directory, LDAP server, or CA SiteMinder.

  Note: Although CA EEM lets you add a user without a password, CA Executive Insight requires that all users have passwords. For more information about setting up users in CA EEM, see the CA EEM documentation.

Identify Options

The installation program prompts you for the following information:

Destination Location

Specifies the path to the location where you want to install the program files. The specified location must be empty.

Default:

- On Windows:

  `C:\Program Files\CA\ExecutiveInsight`

- On Linux:

  `/opt/CA/ExecutiveInsight`

Supporting Components Location

Specifies the full path and name of the supporting components package file. The package file contains software components that are distributed under the GNU Lesser General Public License (LGPL). The name of the package file is as follows:

- On Windows:

  `lgplPackages-win_1.1.zip`

- On Linux:

  `lgplPackages-linux_1.1.tar`

Note: If you download the package file to the same location as the installation program, the program automatically validates the package file.

MySQL Credentials

Specifies the authentication information that is used to connect to your MySQL server. Complete the following fields:

MySQL Server Host Name

Specifies the MySQL host name or IP address.

Default: localhost

Notes:

- By default, MySQL creates the root user account as 'root'@'localhost'. If MySQL is installed on the local system, use the default name, localhost as the host name. If you specify an actual host name or IP address, create a user account on MySQL before installing the product.
- If MySQL is installed on a remote system, set up the DNS on the local system.

  See the section, Configuring MySQL on a Remote System for additional steps.

MySQL Port Number

Specifies the listener port on the MySQL server.

Default: 3306

MySQL Admin User Name

Specifies the MySQL administrator user name.

Default: root

Note: If you do not want to use the default MySQL root user, create a user account on MySQL before installing the product. To create the user account with the required privileges, log in to MySQL as the root user and type the following commands:

```
create user 'admin_user'@'host' identified by 'admin_pwd';
grant Grant option, Select, Insert, Update, Delete, Create, Drop, Reload,
References, Index, Alter, Show Databases, Create Temporary Tables, Lock
Tables, Execute, Create View, Show View, Create Routine, Alter Routine, Create
User, Event, Trigger, Create Tablespace on *.* to 'admin_user'@'host' with
grant option;
flush privileges;
```

admin_user

Defines the administrator user name. Specify this user name in the MySQL Admin User Name option.

host

Specifies the host name or IP address of the MySQL server.

admin_pwd

Defines the password for the administrator user. Specify this password in the MySQL Admin User Password option.

MySQL Admin User Password

Specifies the password for the MySQL administrator user.

Notes:

- If you specified the default localhost as the host name and root as the user name, specify the password that you created during the MySQL installation.
- If you created a user account, specify the password that you defined for the user name (*admin_pwd*).

MySQL Database Credentials

Defines the authentication information that is used to connect to the MySQL database that the installation program created. Complete the following fields:

Database User Name

Defines a database user name. This user must not exist.

Default: execdbadmin

Database User Password

Defines the password for the database user. The password is encrypted.

CA Embedded Entitlements Manager Information

Specifies the authentication information that is used to connect to CA EEM. Complete the following fields:

Host Name

Specified the name of the server that hosts CA EEM.

Administrator Name

Specified the CA EEM administrator user name.

Default: EiamAdmin

Application Name

Specifies the application name used by CA Executive Insight in CA EEM.

Default: ExecutiveInsightForSA

Administrator Password

Specifies the password for the CA EEM administrator user. The password is encrypted.

The installation program registers an application named ExecutiveInsightForSA with CA EEM. The administrator must create users in CA EEM for the application.

Performance Sizing

Consider two factors when sizing the product server:

- The number of business indicators configured
- The maximum number of concurrent users actively requesting data

The number of BIs you configure has a direct effect on the size and performance of the MySQL database and therefore on the CA Executive Insight server.

For more information, see the *MySQL guide* at http://dev.mysql.com/.

Number of Business Indicators	MySQL CPU Cores	MySQL Memory (See Important Note)	MySQL Disk I/O Per Second	CA Executive Insight CPU Cores	MySQL Disk Space
< 500	1	1 GB	100	1	1 GB
500 – 1000	2	1 GB	200	1	2 GB
1000 – 2000	2	1.5 GB	300	2	4 GB
2000 – 3000	3	1.5 GB	400	2	8 GB
3000 - 5000	4	2 GB	600	3	12 GB
5000 - 10000	4	2.4 GB	800	4	16 GB

Important! For optimal memory performance, configure the MySQL property innodb_buffer_pool_size with 150 MB of memory for each 1000 business indicators.

Changing MySQL Sizing on Windows

If you want to adjust the MySQL memory, follow these steps:

1. By default, the MySQL installation creates the configuration file, my.ini under the MySQL installation directory. The default MySQL installation location is C:\Program Files\MySQL\MySQL Server 5.5. If the file does not exist, create one.
2. Update or add the property 'innodb_buffer_pool_size', under the '[mysqld]' section.
3. After updating the configuration file, restart MySQL for the new value to take effect.

Concurrent User Sizing

The number of concurrent users actively accessing the product server affects both the product server and MySQL.

Concurrent Users	CA Executive Insight CPU Cores	CA Executive Insight Memory	MySQL CPU Cores	MySQL Memory
10	1	512 MB	1	1 GB
20	2	512 MB	2	1 GB
30	3	800 MB	3	1.2 GB
40	4	1.2 GB	4	1.5 GB
50	4	1.2 GB	6	2 GB
100	6	1.5 GB	6	2.4 GB

CA APM Server Performance Impact

Once a minute the CA Executive Insight server queries the CA APM server for the business indicator data that has been configured for that connector. More business indicators increase the number of requests increasing CPU use.

To find the number of web service calls and their duration, parse the IntroscopeEnterpriseManager.log file.

Note: For more information about monitoring web services, see the '*CA Application Performance Management Sizing and Performance Guide*'.

Performance varies with each version of CA APM.

- For CA APM 9.0.6, you can monitor the impact of the webservices queries on your CA APM server. Look at the Response Time and Responses Per Interval metrics under the Workstation Investigator Browse tab:

  Custom Metric Agent(Virtual) > Enterprise Manager > WebService > Polling > introscope-web-services/services/MetricsDataService

- For CA APM 9.1 or 9.0 with 500 business indicators, you can expect a 2-second or 3-second spike in CPU use per minute.

Number of BI's per CA APM Connector	CA APM Server CPU Overhead (see Note)	Interval Length (seconds)
< 500	40%	1-3
1000	100%	4-8

2000	200%	8-10
4000	400%	12-16

Note: The CA APM server CPU overhead percentages are relative to one CPU core.

- For releases after CA APM 9.1, you can expect significant improvement in the performance. Support for making bulk web service calls to CA APM was added.

Number of BI's per CA APM Connector	CA APM Server CPU Overhead (see Note)	Interval Length (seconds)
< 500	5%	0.3
1000	10%	0.6
2000	30%	1.0
4000	80%	2.0

Note: The CA APM Server CPU overhead percentages are relative to one CPU core.

To find the number of web service calls and their duration, parse the IntroscopeEnterpriseManager.log file.

- For releases after CA APM 9.1.1, there is session-based authentication for the web service calls from CA Executive Insight to CA APM. Therefore, the periodical authentication calls by CA APM to its authentication provider, such as CA EEM or LDAP, are eliminated.

CA Executive Insight detects the CA APM version that is used for the connector. If you use a version before CA APM 9.1.1, then authentication calls are made for each web service request from CA Executive Insight to CA APM. If you use CA APM 9.1.1 or later, CA Executive Insight is automatically detected session-based authentication is used.

CA SOI Server Performance Impact

Once a minute the CA Executive Insight server queries the CA SOI server for the BI data that has been configured for that connector. These requests can cause an increase in the CPU utilization of the CA SOI server. The utilization increases depending on the number of BIs for that CA SOI connector. A CA SOI instance with 800 to 1500 services can expect a one to three-second spike of 30 percent. This spike percentage is determined on a 2GHz VM in CPU utilization once a minute. Furthermore, the CA Executive Insight web services call results in usage of approximately 300 MB of RAM in the CA SOI server.

Install MySQL on Windows

Note: This installation is only required for a new installation, not an upgrade installation.

CA Executive Insight stores its data in a MySQL database. Before you can install the product, MySQL must be installed. You can install MySQL on the same system as CA Executive Insight or on a remote system.

Note: Before you install MySQL, uninstall any existing installations of MySQL and delete any existing files. See Delete an Older Version of MySQL for more information.

Follow these steps:

1. Double-click mysql-advanced-5.5.8-winx64.msi.

   The Setup Wizard opens.

2. Click Next

   The End-User License Agreement page opens.

3. Accept the license agreement and click Next.

   The Chose Setup Type page opens.

4. Click Complete.

   Note: If you are reinstalling MySQL, click Custom to specify a different install location.

   The Ready to install MySQL Server 5.5 page opens.

5. Click Install.

   The MySQL Enterprise dialog opens.

6. Follow the prompts to start the server instance configuration.

   The Configuration Wizard prompts for a configuration type.

7. Select the Detailed Configuration option button, and click Next.

   The Configuration Wizard prompts for a server type.

8. Select the Develop Machine option button, and click Next.

   The Configuration Wizard prompts for the database usage.

9. Select the Multifunctional Database option button, and click Next.

   The Configuration Wizard prompts for a place to store the InnoDB tablespace.

10. Select \MySQL Datafiles\ from the Installation Path drop-down list, select a drive, and click Next.

    Note: If you reinstall MySQL, remove this directory before rerunning the installer.

    The Configuration Wizard prompts for the number of concurrent connections to the server.

11. Select the Decision Support (DSS)/OLAP option button, and click Next.

    The Configuration Wizard prompts for networking options.

12. Accept the default networking options, and click Next.

    The Configuration Wizard prompts for the default character set.

13. Select the Standard Character Set option button, and click Next.

    The Configuration Wizard prompts for the Windows options.

14. Select the Include Bin Directory in Windows PATH check box, and click Next.

    The Configuration Wizard prompts for the security options.

15. Enter a password in the New root password field. Retype the password in the Confirm field, and click Next.

    The Configuration Wizard prompts to start the configuration.

16. Click Execute.

    The configuration is processed.

17. Click Finish to close the wizard.

    MySQL is installed on Windows. The MySQL service starts automatically.

Important! After you install MySQL, decide whether to update or add the MySQL default configuration, depending on the number of business indicators. For sizing, see Critical CA Executive Insight Sizing Information.

Delete an Older Version of MySQL

Before you install MySQL, uninstall any existing installations of MySQL and delete any existing files by following these steps:

1. Run the MySQL uninstallation from Add/Remove Program.
2. Delete the MySQL system schema files and directory that you entered during MySQL installation, such as the c:\MySQL Datafiles.
3. Delete the MySQL configuration file and directory which is located in the C:\Documents and Settings\All Users\Application Data\MySQL\.
4. Delete the MySQL installation directory which is typically located in the C:\Program Files\MySQL\.

Troubleshooting the MySQL Installation

Configuration Wizard Hangs While Processing the My SQL Configuration on Windows

Symptom:

After the Configuration Wizard starts, it stops responding during the Start service step. The MySQLInstanceConfig.exe and services.exe processes use an excessive amount of CPU.

Solution:

During a successful installation, the Start server step takes a few seconds. If it takes a few minutes, end the configuration process and reinstall MySQL.

To reinstall MySQL:

1. End the MySQLInstanceConfig.exe process using the Windows Task Manager.
2. Uninstall MySQL using Add/Remove Programs.
3. Delete the following directories:

   ```
   C:\Documents and Settings\All Users\Application Data\MySQL
   C:\ProgramData\MySQL
   ```

   Note: These paths have hidden files so you cannot see the files using Windows Explorer.

   To delete the hidden files, open a Command prompt and run the following commands:

   ```
   cd "c:\Documents and settings\All Users\Application Data"
   rmdir /S MySQL
   ```

4. Delete the MySQL data files directory, for example:

   ```
   C:\MySQL Datafiles
   ```

5. (Optional) Remove MySQL from the Windows registry.
6. Reinstall MySQL in a different location, for example:

   ```
   c:\MySQL\MySQL Server 5.5
   ```

   Note: To install MySQL in a different location, select Custom as the setup type.

Configure MySQL on a Remote System

MySQL is typically expected to be installed on the same system where CA Executive Insight is installed. However, CA Executive Insight can connect to a remote MySQL installation. Configure the remote system before proceeding with the product installation.

Follow these steps:

On the remote system where MySQL is installed:

1. Open a command prompt or shell terminal.
2. Type
   `mysql –uroot –p`

   Provide the root password when prompted.
3. At the mysql> command prompt, execute the following commands:
   mysql> `create user '<mysql_admin_user>'@'<ei_hostname>' identified by '<mysql_admin_password>';`

   <mysql_admin_user>

   Specifies the administrator user; typically 'root', but it can be any other named user.

   <ei_hostname>

   Specifies the fully qualified host name or IP address of the system where the product is installed.

   < mysql_admin_password>

   Specified the password for this user.

```
mysql> grant Grant option, Select, Insert, Update, Delete, Create, Drop, Reload,
References, Index, Alter, Show Databases, Create Temporary Tables, Lock Tables,
Execute, Create View, Show View, Create Routine, Alter Routine, Create User,
Event, Trigger, Create Tablespace on *.* to
'<mysql_admin_user>'@'<ei_hostname>'  with grant option;
mysql> flush privileges;
```

When installing the product, enter the above user and password when prompted for the MySQL credentials.

Download the Components Package File for Windows

CA Executive Insight requires some software components that are distributed under the GNU Lesser General Public License (LGPL). Before you install, download the supporting components package file.

Follow these steps:

1. Open your browser and go to the following web page:

   http://opensrcd.ca.com/ips/osgi/ExecutiveInsightForServiceAssurance/V1.1/

   The web page opens.

   Note: The LGPL package has not changed since CA Executive Insight 1.1.

2. Download the lgplPackages-win_1.1.zip file.
3. Copy the zip file to the location where you plan to run the CA Executive Insight installation program.

   Note: If the package file and installation program are in different locations, you are prompted for the location of the package file during the installation process.

   The supporting components package file is downloaded.

Install CA Executive Insight on Windows

You can install CA Executive Insight using an interactive program that lets you change and review your settings before starting the installation process.

Note: If you are doing a base installation, not an upgrade installation, and the previous version of CA Executive Insight installed; uninstall the existing version before installing the new version.

Note: CA Executive Insight does not support Console installation on Windows.

Important! If the installation does not complete successfully, manually delete the schema, cleanup any relevant files, and run the installation program again. See the section, Necessary Cleanup if Installation Doesn't Complete Successfully.

Follow these steps:

1. Download the appropriate files from the CA Support Online website, found at http://ca.com/support.
2. Copy or FTP the zip file to the target system and directory.
3. Extract the installation file using WinZip or a similar utility.
4. Double-click the CA_Executive_Insight-win_<*version*>.exe file, click Next, and accept the license agreement.

5. Continue with the installation by entering the required information.

   Notes:

   - The installation program creates databases named master and tenant1. If you receive an error that a database exists, delete it before continuing the installation. You can delete a database using the drop database command, for example:

     ```
     drop database master;
     ```

   - The installation program creates a user for connecting to the MySQL database. If you receive an error that the user exists, delete it before continuing the installation. You can delete a user using the drop user command, for example:

     ```
     drop user 'execdbadmin'@'localhost';
     ```

   - After you specify the CA EEM credentials, the installation program tests the connection. If a connection cannot be established, an error is displayed. To reenter the credentials, click re-enter. Alternatively, you can click Continue to proceed with the installation using the invalid credentials.

     If you click Continue, configure the CA EEM properties manually before using the product. See modify your CA EEM configuration to make other CA EEM updates.

     For CA EEM12, during CA Executive Insight installation, check whether CA EEM is FIPS enabled or disabled within the CA EEM UI site. For, CA EEM8, the FIPS enabled/disabled value is not required.

   The Notes above only apply to a base installation, not an upgrade installation.

   The CA Executive Insight As Windows Service dialog appears.

6. Specify if you want to create and automatically start the CA Executive Insight process as a Windows service. By default, both options are selected which assumes you want to automatically create and start the service.

   If you decide to *not* create the Windows service, start the product by running the Executive_Insight_For_SA.exe executable that is located within the installation directory. Double-click the file or run it from the command line. A Command prompt window launches. To stop the product, close the Comment prompt window.

   If you decide to create the Windows service, you can start or stop the product using Services.

   The Review Settings dialog opens as the last dialog before the installation process begins.

7. Review the settings and use the Previous button to change the values you entered.

8. Click Install to begin the installation.

   The installation process begins, and the progress is displayed.

9. Click Finish when the installation completes.

   The installation program exits. CA Executive Insight is installed on Windows.

   Note: ExecutiveInsight_Install.log is located in the log subdirectory of the installation directory.

Necessary Cleanup if Installation Does Not Complete Successfully

After the installer starts installing the files, do not kill the process. This can lead to a corruption of files and potentially the database schemas. Allow the installation to compete and then run the uninstaller to uninstall the product. If the installer is interrupted, perform the following steps:

1. Drop the MySQL master database.
2. Drop MySQL tenant1 database.
3. Drop MySQL user – execDbAdmin.
4. Delete the ExecutiveInsight installation folder.

Start/Stop the CA Executive Insight Server on Windows

If you chose to create the Windows service and start CA Executive Insight automatically, then run the product after the install program. However, if you chose to create the Windows service and *not* start it automatically, then start the program manually.

To start CA Executive Insight server from service

1. From the service tab in task manager, select 'CA Executive Insight for Service Assurance'.
2. Click the start button.

   The CA Executive Insight server starts.

To start CA Executive Insight server on Windows manually

1. Verify that the MySQL service is running.
2. Double-click the following file:
   `install_dir\Executive_Insight_For_SA.exe`

   install_dir

   Specifies the directory where CA Executive Insight is installed.

   The CA Executive Insight server starts.

To stop CA Executive Insight server from service

1. From the service tab in task manager, select 'CA Executive Insight for Service Assurance'.
2. Click the stop button.

   The CA Executive Insight server stops.

To stop CA Executive Insight server process

1. Close the Command prompt window that is launched by Executive_Insight_For_SA.exe.
2. The CA Executive Insight server stops.

Examine Log Files (Optional)

Verify proper CA Executive Insight installation by checking the log files.

- You can view the install/upgrade log file in the log directory in the installation directory.
- A log file named ei_inst_history.txt lists details of the installation/upgrade history in your environment. The file contains specific details about the version you upgraded or installed and whether the process was successful. The file is located under install.dir.

Log in to the Admin UI

To verify the installation, log in to the Admin UI using a browser.

Follow these steps:

1. Open your browser and go to the following web page:

   `http://host_address:8080/admin`

   host_address

   The host name or IP address of the computer where you installed CA Executive Insight.
2. Enter the credentials of the CA Executive Insight user. The user was configured directly in CA EEM or in the AD/LDAP/SiteMinder system with which CA EEM has been configured to connect.
3. Click Log In.

Log in to the Mobile Application

After you complete the installation, log in to the mobile application using a browser. On an iPad or iPhone, use the Safari browser. On Android devices, for Android 2.3, use the default Android browser. For Android 4.0 and 4.1, use the Chrome browser.

Follow these steps:

1. Open your browser and go to the following web page:

   `http://host_address:8080/`

   host_address

   Specifies the host name or IP address of the computer where you installed CA Executive Insight.

2. Enter the credentials of the CA Executive Insight user. The user was configured directly in CA EEM or in the AD/LDAP/SiteMinder system with which CA EEM has been configured to connect.
3. Click Log In.

Important! If you are running CA Executive Insight on the mobile device, refresh the application after the upgrade is complete. A refreshed application ensures that the latest version is running on your mobile device. The refresh is done by restarting the browser session running the application or relaunching the application from the shortcut on supported devices.

Chapter 4: Install CA Executive Insight on Linux

Install CA Executive Insight on Linux

CA Executive Insight supports *business indicators* that are mapped to IT metrics. You create business indicators that are based on the available metrics from different data sources in your environment such as CA APM.

A *metric connector* creates a connection between a data source and the CA Executive Insight application. After the connection is established, the application retrieves IT metrics from the data source and publishes the metric data as business indicators in a dashboard.

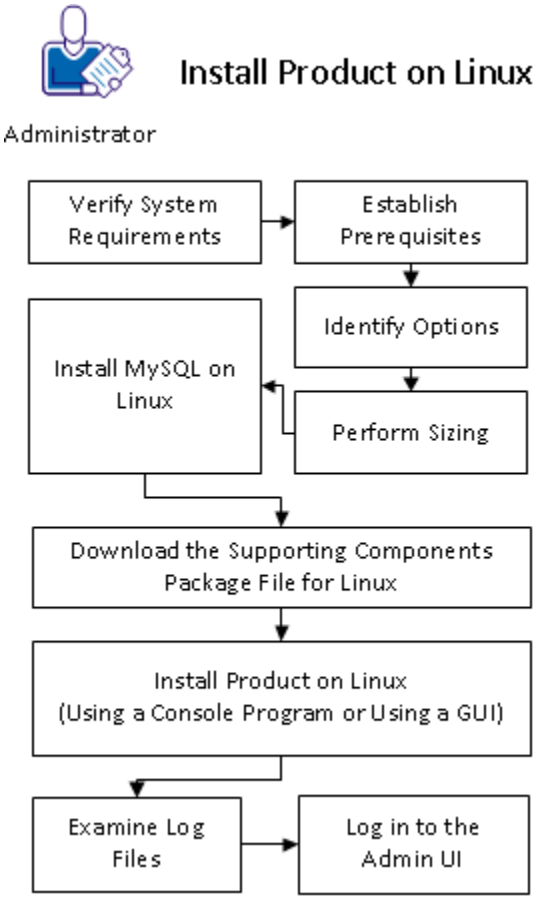
Many data sources are supported:

- CA Application Performance Management (CA APM)
- CA Service Operations Insight (CA SOI)
- CA Capacity Command Center (CA CCC)
- Comma-separated values files (CSV files)
- Web services connectors

To retrieve data, add a connector and specify the connection information for the instance.

Before you configure metric connectors and build business indicators for your mobile device users, complete the installation of CA Executive Insight.

The following illustration describes how an administrator installs CA Executive Insight on a Linux host.



To complete the installation of CA Executive Insight on Linux, follow these steps:

1. Prepare for installation.
   - Verify system requirements (see page 13)
   - Establish prerequisites (see page 15)
   - Identify options (see page 15)
   - Perform sizing (see page 18)
   - Install MySQL on Linux (see page 41)
2. Install the product.
   - Download the supporting components package file for Linux (see page 43)
   - Install CA Executive Insight on Linux (see page 43)

3. Post-installation procedures.
   - Examine Log Files (see page 47)
   - Log in to the Admin UI (see page 28)

Verify System Requirements

Verify that the following system requirements are filled before you install CA Executive Insight:

Server Requirements

The following platforms are supported:

- Windows 2008 64-bit
- Linux Red Hat 5 and Red Hat 6 64-bit

Data Source Requirements

The following CA Technologies product versions are supported:

- CA APM 9.0.x and 9.1.x

  CA Executive Insight can retrieve CA Introscope® metrics from an Enterprise Manager in a standalone environment or a Manager of Managers (MOM) Enterprise Manager in a clustered environment. If the APM instance is connected to Transaction Impact Monitors (TIMs), Customer Experience metrics also are available.

- CA Introscope® 8.1.1, 8.2, 9.0.x and 9.1.x

  CA Executive Insight can retrieve CA Introscope® metrics from an Enterprise Manager in a standalone environment or a MOM Enterprise Manager in a clustered environment.

- CA CEM 4.5

  CA Executive Insight can retrieve customer experience metrics from a Customer Experience Manager instance.

- CA Service Operations Insight 3.0

  CA Executive Insight can retrieve the business service hierarchy and service metrics from CA SOI.

- CA Capacity Command Center 2.1.0

  CA Executive Insight can retrieve the group hierarchy from CA Capacity Command Center and the corresponding efficiency metrics.

Mobile Requirements

CA Executive Insight is a web application that is designed to run on any mobile platform with a browser that supports WebKit. The supported browsers include Safari, Google Chrome, or Android.

CA Executive Insight is certified on the following mobile devices:

- Android 7 and 10-inch tablets running Android OS 4.x, such as Google Nexus 7 running Android 4.1 and Samsung Galaxy Tab 2 running Android 4.0 with the Chrome browser.
- Apple iPhone 4, iPhone 4S, and iPhone5 running the Safari browser with iOS 6.1.
- Apple iPad 2, iPad 3, and iPad 4 running the Safari browser with iOS 6.1.

  Note: CA Executive Insight 2.0 and 1.3 do not support iPad 1.
- Smartphones running Android 2.3 such as HTC Incredible 2 running the default Android browser that is shipped with the OS.
- Smartphones running Android 4.x, such as Samsung S2 or Samsung S3, Samsung Galaxy Nexus, with the Chrome browser.

  Note: CA Executive Insight 1.3 and 2.0 do not support Blackberry Playbook.

CA Executive Insight supports administrators running the mobile user interface on the following desktop browsers:

- Safari 5.1.x
- Google Chrome 25.x

  Note: The preceding platforms have been certified at the time of General Availability (GA). Given rapidly changing technology, for current information regarding platform support, see the CA Executive Insight Support web page at http://ca.com/support.

Admin UI Browser Requirements

To administer CA Executive Insight, log in to the Admin UI using a browser.

The Admin UI is certified on the following browsers:

- Internet Explorer 8 and 9
- Firefox 19.x

Note: The preceding browsers have been certified at the time of General Availability (GA). Given rapidly changing technology, for current information regarding browser support, see the CA Executive Insight Support web page at http://ca.com/support.

Supported Security Standards

CA Executive Insight complies with the FIPS 140-2 standard.

Establish Prerequisites

Before you install the product, review the following requirements:

- MySQL Enterprise Edition 5.5.8

  The product stores its data in a MySQL database. The required MySQL packages are provided with the product, install them separately. You do not need to reinstall MySQL when upgrading from an older version of the product.

- CA Embedded Entitlements Manager (CA EEM) 8.4 or 12.0

  CA EEM is used to authenticate and authorize the users that log in to CA Executive Insight. Before you can log in to CA Executive Insight, set up a user in CA EEM. To set up a user, create a user in the CA EEM local store. Alternatively, you can configure CA EEM to connect to your Active Directory, LDAP server, or CA SiteMinder.

  Note: Although CA EEM lets you add a user without a password, CA Executive Insight requires that all users have passwords. For more information about setting up users in CA EEM, see the CA EEM documentation.

Identify Options

The installation program prompts you for the following information:

Destination Location

Specifies the path to the location where you want to install the program files. The specified location must be empty.

Default:

- On Windows:

  `C:\Program Files\CA\ExecutiveInsight`

- On Linux:

  `/opt/CA/ExecutiveInsight`

Supporting Components Location

Specifies the full path and name of the supporting components package file. The package file contains software components that are distributed under the GNU Lesser General Public License (LGPL). The name of the package file is as follows:

- On Windows:

  `lgplPackages-win_1.1.zip`

- On Linux:

  `lgplPackages-linux_1.1.tar`

Note: If you download the package file to the same location as the installation program, the program automatically validates the package file.

MySQL Credentials

Specifies the authentication information that is used to connect to your MySQL server. Complete the following fields:

MySQL Server Host Name

Specifies the MySQL host name or IP address.

Default: localhost

Notes:

- By default, MySQL creates the root user account as 'root'@'localhost'. If MySQL is installed on the local system, use the default name, localhost as the host name. If you specify an actual host name or IP address, create a user account on MySQL before installing the product.
- If MySQL is installed on a remote system, set up the DNS on the local system.

  See the section, Configuring MySQL on a Remote System for additional steps.

MySQL Port Number

Specifies the listener port on the MySQL server.

Default: 3306

MySQL Admin User Name

Specifies the MySQL administrator user name.

Default: root

Note: If you do not want to use the default MySQL root user, create a user account on MySQL before installing the product. To create the user account with the required privileges, log in to MySQL as the root user and type the following commands:

```
create user 'admin_user'@'host' identified by 'admin_pwd';
grant Grant option, Select, Insert, Update, Delete, Create, Drop, Reload,
References, Index, Alter, Show Databases, Create Temporary Tables, Lock
Tables, Execute, Create View, Show View, Create Routine, Alter Routine, Create
User, Event, Trigger, Create Tablespace on *.* to 'admin_user'@'host' with
grant option;
flush privileges;
```

admin_user

Defines the administrator user name. Specify this user name in the MySQL Admin User Name option.

host

Specifies the host name or IP address of the MySQL server.

admin_pwd

Defines the password for the administrator user. Specify this password in the MySQL Admin User Password option.

MySQL Admin User Password

Specifies the password for the MySQL administrator user.

Notes:

- If you specified the default localhost as the host name and root as the user name, specify the password that you created during the MySQL installation.
- If you created a user account, specify the password that you defined for the user name (*admin_pwd*).

MySQL Database Credentials

Defines the authentication information that is used to connect to the MySQL database that the installation program created. Complete the following fields:

Database User Name

Defines a database user name. This user must not exist.

Default: execdbadmin

Database User Password

Defines the password for the database user. The password is encrypted.

CA Embedded Entitlements Manager Information

Specifies the authentication information that is used to connect to CA EEM. Complete the following fields:

Host Name

Specified the name of the server that hosts CA EEM.

Administrator Name

Specified the CA EEM administrator user name.

Default: EiamAdmin

Application Name

Specifies the application name used by CA Executive Insight in CA EEM.

Default: ExecutiveInsightForSA

Administrator Password

Specifies the password for the CA EEM administrator user. The password is encrypted.

The installation program registers an application named ExecutiveInsightForSA with CA EEM. The administrator must create users in CA EEM for the application.

Performance Sizing

Consider two factors when sizing the product server:

- The number of business indicators configured
- The maximum number of concurrent users actively requesting data

The number of BIs you configure has a direct effect on the size and performance of the MySQL database and therefore on the CA Executive Insight server.

For more information, see the *MySQL guide* at http://dev.mysql.com/.

Number of Business Indicators	MySQL CPU Cores	MySQL Memory (See Important Note)	MySQL Disk I/O Per Second	CA Executive Insight CPU Cores	MySQL Disk Space
< 500	1	1 GB	100	1	1 GB
500 – 1000	2	1 GB	200	1	2 GB
1000 – 2000	2	1.5 GB	300	2	4 GB
2000 – 3000	3	1.5 GB	400	2	8 GB
3000 - 5000	4	2 GB	600	3	12 GB
5000 - 10000	4	2.4 GB	800	4	16 GB

Important! For optimal memory performance, configure the MySQL property innodb_buffer_pool_size with 150 MB of memory for each 1000 business indicators.

Changing MySQL Sizing on Linux

To adjust the MySQL memory, follow these steps:

- By default, the MySQL installation does not create the configuration file, my.cnf. In this case, create it under /etc. If the file exists, update it based on your business needs.
- Update or add the entry 'innodb_buffer_pool_size' under the '[mysqld]' section.
- After updating the configuration file, restart MySQL for the new value to take effect.

Concurrent User Sizing

The number of concurrent users actively accessing the product server affects both the product server and MySQL.

Concurrent Users	CA Executive Insight CPU Cores	CA Executive Insight Memory	MySQL CPU Cores	MySQL Memory
10	1	512 MB	1	1 GB
20	2	512 MB	2	1 GB
30	3	800 MB	3	1.2 GB
40	4	1.2 GB	4	1.5 GB
50	4	1.2 GB	6	2 GB
100	6	1.5 GB	6	2.4 GB

CA APM Server Performance Impact

Once a minute the CA Executive Insight server queries the CA APM server for the business indicator data that has been configured for that connector. More business indicators increase the number of requests increasing CPU use.

To find the number of web service calls and their duration, parse the IntroscopeEnterpriseManager.log file.

Note: For more information about monitoring web services, see the '*CA Application Performance Management Sizing and Performance Guide*'.

Performance varies with each version of CA APM.

- For CA APM 9.0.6, you can monitor the impact of the webservices queries on your CA APM server. Look at the Response Time and Responses Per Interval metrics under the Workstation Investigator Browse tab:

  Custom Metric Agent(Virtual) > Enterprise Manager > WebService > Polling > introscope-web-services/services/MetricsDataService
- For CA APM 9.1 or 9.0 with 500 business indicators, you can expect a 2-second or 3-second spike in CPU use per minute.

Number of BI's per CA APM Connector	CA APM Server CPU Overhead (see Note)	Interval Length (seconds)
< 500	40%	1-3
1000	100%	4-8

2000	200%	8-10
4000	400%	12-16

Note: The CA APM server CPU overhead percentages are relative to one CPU core.

- For releases after CA APM 9.1, you can expect significant improvement in the performance. Support for making bulk web service calls to CA APM was added.

Number of BI's per CA APM Connector	CA APM Server CPU Overhead (see Note)	Interval Length (seconds)
< 500	5%	0.3
1000	10%	0.6
2000	30%	1.0
4000	80%	2.0

Note: The CA APM Server CPU overhead percentages are relative to one CPU core.

To find the number of web service calls and their duration, parse the IntroscopeEnterpriseManager.log file.

- For releases after CA APM 9.1.1, there is session-based authentication for the web service calls from CA Executive Insight to CA APM. Therefore, the periodical authentication calls by CA APM to its authentication provider, such as CA EEM or LDAP, are eliminated.

CA Executive Insight detects the CA APM version that is used for the connector. If you use a version before CA APM 9.1.1, then authentication calls are made for each web service request from CA Executive Insight to CA APM. If you use CA APM 9.1.1 or later, CA Executive Insight is automatically detected session-based authentication is used.

CA SOI Server Performance Impact

Once a minute the CA Executive Insight server queries the CA SOI server for the BI data that has been configured for that connector. These requests can cause an increase in the CPU utilization of the CA SOI server. The utilization increases depending on the number of BIs for that CA SOI connector. A CA SOI instance with 800 to 1500 services can expect a one to three-second spike of 30 percent. This spike percentage is determined on a 2GHz VM in CPU utilization once a minute. Furthermore, the CA Executive Insight web services call results in usage of approximately 300 MB of RAM in the CA SOI server.

Install MySQL on Linux

Note: This is only required for a new installation, not an upgrade installation.

CA Executive Insight stores its data in a MySQL database. Before you can install the product, MySQL must be installed. You can install MySQL on the same system as CA Executive Insight or on a remote system.

Note: Before you install MySQL, uninstall any existing installations of MySQL and delete any existing files.

Follow these steps:

1. Log in as root.
2. Enter the following command to list the MySQL packages installed on your system:

   ```
   rpm -qa | grep -i mysql
   ```

   If the results of this command show you have an existing installation of MySQL, remove the MySQL packages:

   a. Enter the following command to remove the installed packages:

      ```
      rpm -e packagename
      ```

      packagename

      Specifies the name of the package that you want to remove.

      Run the command for each package listed in Step 2.

      Note: You can forcefully remove a package by typing the following command:

      ```
      rpm –e --allmatches packagename --nodeps
      ```

   b. Remove the MySQL system schema files, which are located in the /var/lib/mysql/mysql directory. Delete this directory.

   c. Remove the MySQL configuration file, which is located in the /etc/my.cnf (or other location that the user created).

3. Enter the following command to install the MySQL server:

   ```
   rpm -i MySQL-server-advanced-5.5.8-1.rhel5.x86_64.rpm
   ```

4. Enter the following command to install the MySQL client:

   ```
   rpm -i MySQL-client-advanced-5.5.8-1.rhel5.x86_64.rpm
   ```

5. Enter the following command to start the MySQL database:

   ```
   /etc/init.d/mysql start
   ```

6. Enter the following command to create a password:

   ```
   mysqladmin -u root password
   ```

   You are prompted to enter a password.

7. Enter your password.

   The password is masked.

8. Enter the following command to log in to the database with the new password:

   ```
   mysql -h localhost -u root –p
   ```

   You are prompted to enter a password.

9. Enter your password.

   The password is masked.

Important! After installing the MySQL, and based on the number of business indicators; decide whether the MySQL default configuration needs to be updated or added. See Critical CA Executive Insight Sizing Information for sizing considerations.

Configure MySQL on a Remote System

MySQL is typically expected to be installed on the same system where CA Executive Insight is installed. However, CA Executive Insight can connect to a remote MySQL installation. Configure the remote system before proceeding with the product installation.

Follow these steps:

On the remote system where MySQL is installed:

1. Open a command prompt or shell terminal.
2. Type
   ```
   mysql –uroot –p
   ```
   Provide the root password when prompted.
3. At the mysql> command prompt, execute the following commands:
   ```
   mysql> create user ‘<mysql_admin_user>’@'<ei_hostname>' identified by '<
   mysql_admin_password>';
   ```

   <mysql_admin_user>

   Specifies the administrator user; typically ‘root’, but it can be any other named user.

   <ei_hostname>

   Specifies the fully qualified host name or IP address of the system where the product is installed.

< mysql_admin_password>

Specified the password for this user.

```
mysql> grant Grant option, Select, Insert, Update, Delete, Create, Drop, Reload,
References, Index, Alter, Show Databases, Create Temporary Tables, Lock Tables,
Execute, Create View, Show View, Create Routine, Alter Routine, Create User,
Event, Trigger, Create Tablespace on *.* to
'<mysql_admin_user>'@'<ei_hostname>'  with grant option;
mysql> flush privileges;
```

When installing the product, enter the above user and password when prompted for the MySQL credentials.

Download the Components Package File for Linux

CA Executive Insight requires some software components that are distributed under the GNU Lesser General Public License (LGPL). Before you install, download the supporting components package file.

Follow these steps:

1. Open your browser and go to the following web page:

   http://opensrcd.ca.com/ips/osgi/ExecutiveInsightForServiceAssurance/V1.1/

   The web page opens.

   Note: The LGPL package has not changed since CA Executive Insight 1.1.

2. Download the lgplPackages-linux_1.1.tar file.

3. Copy or FTP the tar file to the location where you plan to run the CA Executive Insight installation program.

   Note: If the package file and installation program are in different locations, you are prompted for the location of the package file during the installation process.

   The supporting components package file is downloaded.

Install CA Executive Insight on Linux Using a Console Program

You can install the CA Executive Insight using an interactive console program.

Note: If you are doing a base installation, and not an upgrade installation, and have a previous version of CA Executive Insight installed on your system; you must uninstall the existing version prior to installing the new version.

Important! If the installation does not complete successfully, you must manually delete the schema, cleanup any relevant files, and run the installation again. See the section, Necessary Cleanup if Installation Doesn't Complete Successfully.

Follow these steps:

1. Log in as root.
2. Download the appropriate file from the CA Support Online website, found at http://ca.com/support.
3. Copy or FTP the tar file to the target system and directory.
4. Enter the following command to extract the installation file:

   `tar -xvf CA_Executive_Insight-linux_installer_<version>.tar`
5. Enter the following command to obtain execute permission for the install file:

   `chmod +x CA_Executive_Insight-linux_<version>.bin`
6. Enter the following command to start the installation:

   `./CA_Executive_Insight-linux_<I>.bin -i console`

   The installation program opens.
7. Press Enter and accept the license agreement.
8. Continue with the installation by entering the required information.

   Notes:

   - The installation program creates databases named master and tenant1. If you receive an error that a database exists, you must delete it before continuing the installation. You can delete a database using the drop database command, for example:

     `drop database master;`
   - The installation program creates a user for connecting to the MySQL database. If you receive an error that the user exists, you must delete it before continuing the installation. You can delete a user using the drop user command, for example:

     `drop user 'execdbadmin'@'localhost';h`
   - After you specify the CA EEM credentials, the installation program tests the connection. If a connection cannot be established, an error is displayed. To reenter the credentials, enter 1. Alternatively, you can enter 2 to proceed with the installation using the invalid credentials.

     If you enter 2, you must configure the CA EEM properties manually before using the product. See modify your CA EEM configuration to make other CA EEM updates.

   The Notes above only apply to a base installation, not an upgrade installation.

   The installation settings are listed before the installation process begins.

9. Press Enter to begin the installation.

   The installation process begins, and the progress is displayed.

10. Press Enter when the installation completes.

    The installation program exits. CA Executive Insight is installed on Linux.

    Note: ExecutiveInsight_Install.log is located in the log subdirectory of the installation directory.

Install CA Executive Insight on Linux Using a GUI

You can install the CA Executive Insight using a GUI that lets you change and review your settings before starting the installation process.

Note: To use the graphical installation, X11 must be set up on your system. If X11 is not set up, the installation program runs in console mode instead.

Note: If you are doing a base installation, and not an upgrade installation, and have a previous version of CA Executive Insight installed on your system; you must uninstall the existing version prior to installing the new version.

Important! If the installation does not complete successfully, you must manually delete the schema, cleanup any relevant files, and run the installation program again. See the section, Necessary Cleanup if Installation Doesn't Complete Successfully.

Follow these steps:

1. Log in as root or as a user having root level privileges.
2. Download the appropriate file from the CA Support Online website, found at http://ca.com/support.
3. Copy or FTP the tar file to the target system and directory.
4. Enter the following command to extract the installation file:

   `tar -xvf CA_Executive_Insight-linux_installer_<version>.tar`

5. Enter the following command to obtain execute permission for the install file:

   `chmod +x CA_Executive_Insight-linux_<version>.bin`

6. Enter the following command to start the installation:

   `./CA_Executive_Insight-linux_<version>.bin -i GUI`

   The installation program opens.

7. Click Next and accept the license agreement.

8. Continue with the installation by entering the required information.

   Notes:

   - The installation program creates databases named master and tenant1. If you receive an error that a database exists, you must delete it before continuing the installation. You can delete a database using the drop database command, for example:

     ```
     drop database master;
     ```

   - The installation program creates a user for connecting to the MySQL database. If you receive an error that the user exists, you must delete it before continuing the installation. You can delete a user using the drop user command, for example:

     ```
     drop user 'execdbadmin'@'localhost';
     ```

   - After you specify the CA EEM credentials, the installation program tests the connection. If a connection cannot be established, an error is displayed. To reenter the credentials, click Re-enter. Alternatively, you can click Continue to proceed with the installation using the invalid credentials.

     If you click Continue, you must configure the CA EEM properties manually before using the product. See modify your CA EEM configuration to make other CA EEM updates.

   The Notes above only apply to a base installation, not an upgrade installation.

   The Review Settings dialog opens as the last dialog before the installation process begins.

9. Review the settings and use the Previous button to change the values you entered.

10. Click Install to begin the installation.

    The installation process begins, and the progress is displayed.

11. Click Finish when the installation completes.

    The installation program exits. CA Executive Insight is installed on Linux.

    Note: ExecutiveInsight_Install.log is located in the log subdirectory of the installation directory.

Necessary Cleanup if Installation Does Not Complete Successfully

After the installer starts installing the files, do not kill the process. This can lead to a corruption of files and potentially the database schemas. Allow the installation to compete and then run the uninstaller to uninstall the product. If the installer is interrupted, perform the following steps:

1. Drop the MySQL master database.
2. Drop MySQL tenant1 database.

3. Drop MySQL user – execDbAdmin.
4. Delete the ExecutiveInsight installation folder.

Start/Stop the CA Executive Insight Server on Linux

To use CA Executive Insight, you issue a command to run a script that starts/stops the server.

Follow these steps:

1. Verify that MySQL is running.
2. Change to the following directory at the command prompt:

   install_dir/bin/

   install_dir

   Specifies the directory where CA Executive Insight is installed.
3. To start the server, enter the following command:

   ```
   ./ServerAndUI.sh start
   ```

   The CA Executive Insight server starts.
4. To stop the server, enter the following command:

   ```
   ./ServerAndUI.sh stop
   ```

   The CA Executive Insight server stops.

Examine Log Files (Linux Optional)

Verify proper CA Executive Insight installation by checking the log files.

- You can view the install/upgrade log file in the log directory in the installation directory.
- A log file named ei_inst_history.txt lists details of the installation/upgrade history in your environment. The file contains specific details about the version you upgraded or installed and whether the process was successful. The file is located under install.dir.

Log in to the Admin UI

To verify the installation, log in to the Admin UI using a browser.

Follow these steps:

1. Open your browser and go to the following web page:

   `http://host_address:8080/admin`

   host_address

   The host name or IP address of the computer where you installed CA Executive Insight.

2. Enter the credentials of the CA Executive Insight user. The user was configured directly in CA EEM or in the AD/LDAP/SiteMinder system with which CA EEM has been configured to connect.
3. Click Log In.

Log in to the Mobile Application

After you complete the installation, log in to the mobile application using a browser. On an iPad or iPhone, use the Safari browser. On Android devices, for Android 2.3, use the default Android browser. For Android 4.0 and 4.1, use the Chrome browser.

Follow these steps:

1. Open your browser and go to the following web page:

   `http://host_address:8080/`

   host_address

   Specifies the host name or IP address of the computer where you installed CA Executive Insight.

2. Enter the credentials of the CA Executive Insight user. The user was configured directly in CA EEM or in the AD/LDAP/SiteMinder system with which CA EEM has been configured to connect.
3. Click Log In.

Important! If you are running CA Executive Insight on the mobile device, refresh the application after the upgrade is complete. A refreshed application ensures that the latest version is running on your mobile device. The refresh is done by restarting the browser session running the application or relaunching the application from the shortcut on supported devices.

Chapter 5: Upgrade CA Executive Insight

Upgrade Support

CA Executive Insight supports:

- Direct upgrade for the last two previous major or minor releases

  Example: You can upgrade from 1.2 and 1.3 to 2.0.

- Successive upgrades (for older releases)

  Example: To upgrade from 1.1 to 2.0, you must upgrade from 1.1 to 1.3, and from 1.3 to 2.0.

Upgrades include product files and the database.

Upgrade Considerations

Upon initializing a CA Executive Insight installation, CA Executive Insight installation program automatically identifies if you are performing an upgrade installation. The upgrade installation program automatically acquires and verifies the following CA Executive Insight variables such as location, database schema, CA EEM information. The upgrade program does not require you to enter this information. However, the upgrade installation asks for acceptance of all license agreements, supporting component location, and whether to configure CA Executive Insight as a Windows service (on Windows).

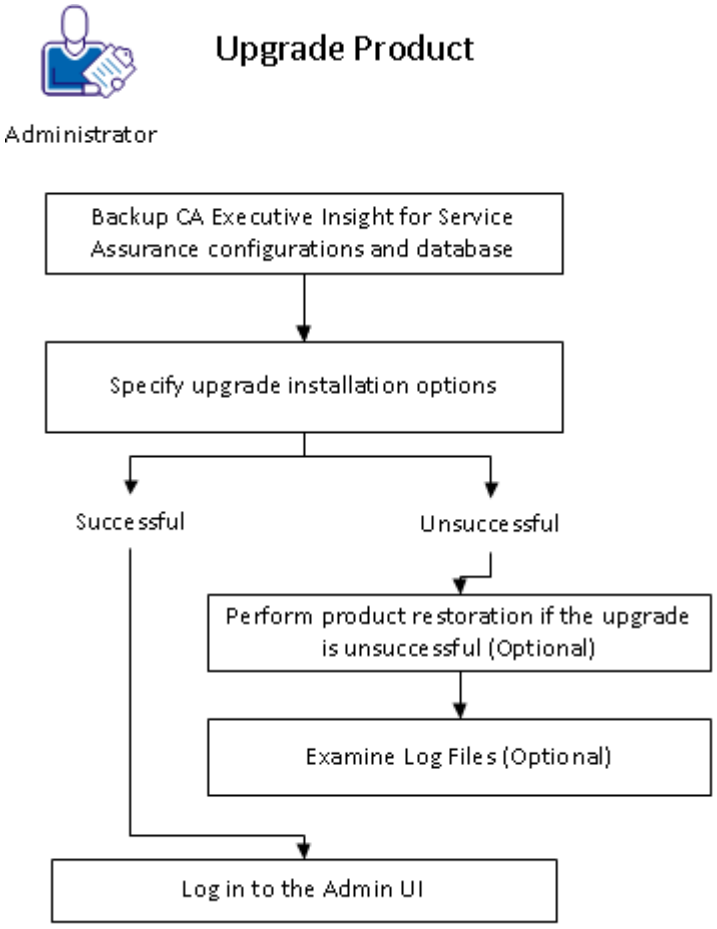
Important! Ensure the existing CA Executive Insight functions correctly before proceeding with an upgrade installation.

Important! Create a back-up of the CA Executive Insight installation location and the database. In the unlikely event that the upgrade fails, without all parts of CA Executive Insight upgraded, you would need to restore the previous version's files and schema.

Begin the Installation process as described. CA Executive Insight automatically begins and during the introduction identifies it is an upgrade and specifies the source and target versions of the upgrade.

Important! After performing an upgrade, refresh your application and log in again. If there is an open session in the mobile user interface or the administration user interface, without a refresh, error messages with garbled characters may display on the login page.

The following illustration describes how an administrator performs an installation upgrade.



To complete the upgrade installation of CA Executive Insight, follow these steps:

1. Backup the CA Executive Insight configurations and database (see page 51)
2. Specify upgrade installation options (see page 52)
3. If successful, Log in to the Admin UI (see page 53)
4. If unsuccessful:
    a. Perform product restoration if the upgrade is unsuccessful (Optional) (see page 52)
    b. Examine Log Files (Optional) (see page 28)

Backup the CA Executive Insight Configurations and Database

To create the backup, copy the files in the installation directory to a backup directory. Then, export the database using the mysqldump utility, which is normally located in the mysql/bin directory. Once the files and database are backed up, you can then restore CA Executive Insight.

If the upgrade should fail, this process creates back-up files that could be utilized to restore CA Executive Insight.

Follow these steps:

1. Stop CA Executive Insight.
2. Create a new directory to contain the backed up CA Executive Insight configuration files.
3. Copy the config subdirectory within the directory where CA Executive Insight is installed into your newly created backup directory.

   The default installation location on Windows is C:\Program Files\CA\ExecutiveInsight.

   The default installation location on Linux is /opt/CA/ExecutiveInsight.
4. Open the terminal/Command Prompt.
5. Point the terminal to the directory which has the MySQL binaries.

   For Windows, by default, it is:

   ```
   c:\Program Files\MySQL\MySQL Server 5.5\bin
   ```

   For Linux, by default, it is:

   ```
   c:\Program Files\MySQL\MySQL Server 5.5\usr\bin
   ```
6. To export your schema, enter the following commands and your MySQL passwords when prompted:

   ```
   mysqldump -p --user=<username> --add-drop-table master >
   <backupdir>\masterbackup.bin
   mysqldump -p --user=<username> --add-drop-table tenant1 >
   <backupdir>\tenant1backup.bin
   ```

   - <username> is the MySQL username of the user that is being used for CA Executive Insight schemas (default is execdbadmin).
   - <backupdir> is the directory where you want to store the backup files.

   If the MySQL programs are not in your path, manually specify the location of the mysqldump program in your commands.

   A backed up copy of CA Executive Insight is created.

Specify Upgrade Installation Options

During the upgrade installation process, some steps are not displayed as they are already known from the previous CA Executive Insight installation.

The interactive CA Executive Insight upgrade installation program prompts you for the following information:

MySQL Credentials

These are the credentials that are required to connect to the MySQL database. The user specified is the MySQL root user or a MySQL user with administrative privileges.

Supporting Components Location

Specifies the full path to and name of the supporting components package file. The package file contains software components that are distributed under the GNU Lesser General Public License (LGPL). The name of the package file is as follows:

- On Windows:
  `lgplPackages-win_1.1.zip`
- On Linux:
  `lgplPackages-linux_1.1.tar`

  Note: If you download the package file to the same location as the installation program, it validates the package file without prompting for it.

Once the information is provided the upgrade installer continues with the upgrade. After a successful upgrade, validate that the application can be accessed and whether all data has been preserved.

Perform Product Restoration if the Upgrade is Unsuccessful (Optional)

You can restore CA Executive Insight back to the previous version, in the unlikely event that the upgrade fails.. This process creates a restoration of the product.

Follow these steps:

1. Uninstall all versions of CA Executive Insight that are currently installed. The product uninstall program drops the databases master and tenant1. If the un-install fails, manually clean up the master and tenant database schemas using the MySQL commands as follows:
   ```
   drop database master;
   drop database tenant1;
   ```
2. Install the version of CA Executive Insight you want to restore.
3. Stop CA Executive Insight.

4. Import the schema by entering the following commands:

   ```
   mysql -u <username> -p --database=master < <backupdir>\masterbackup.bin
   mysql -u <username> -p --database=tenant1 < <backupdir>\tenantbackup.bin
   ```

   - <username> is the MySQL username that is used with CA Executive Insight.

     Note: This Username should be the same person who took the backup.

   - <backupdir> is pointing to the path where your binary schema backup files are located.

   - Enter your passwords for your MySQL user when prompted.

5. Copy the backed-up configuration files into the config directory, replacing files if necessary.

6. Start CA Executive Insight.

   A restored version of the product has been created.

Examine Log Files (Optional)

Verify proper CA Executive Insight installation by checking the log files.

- You can view the install/upgrade log file in the log directory in the installation directory.
- A log file named ei_inst_history.txt lists details of the installation/upgrade history in your environment. The file contains specific details about the version you upgraded or installed and whether the process was successful. The file is located under install.dir.

Log in to the Admin UI

To verify the installation, log in to the Admin UI using a browser.

Follow these steps:

1. Open your browser and go to the following web page:

   `http://host_address:8080/admin`

   host_address

   The host name or IP address of the computer where you installed CA Executive Insight.

2. Enter the credentials of the CA Executive Insight user. The user was configured directly in CA EEM or in the AD/LDAP/SiteMinder system with which CA EEM has been configured to connect.

3. Click Log In.

Log in to the Mobile Application

After you complete the installation, log in to the mobile application using a browser. On an iPad or iPhone, use the Safari browser. On Android devices, for Android 2.3, use the default Android browser. For Android 4.0 and 4.1, use the Chrome browser.

Follow these steps:

1. Open your browser and go to the following web page:

   `http://host_address:8080/`

   host_address

   Specifies the host name or IP address of the computer where you installed CA Executive Insight.

2. Enter the credentials of the CA Executive Insight user. The user was configured directly in CA EEM or in the AD/LDAP/SiteMinder system with which CA EEM has been configured to connect.

3. Click Log In.

Important! If you are running CA Executive Insight on the mobile device, refresh the application after the upgrade is complete. A refreshed application ensures that the latest version is running on your mobile device. The refresh is done by restarting the browser session running the application or relaunching the application from the shortcut on supported devices.

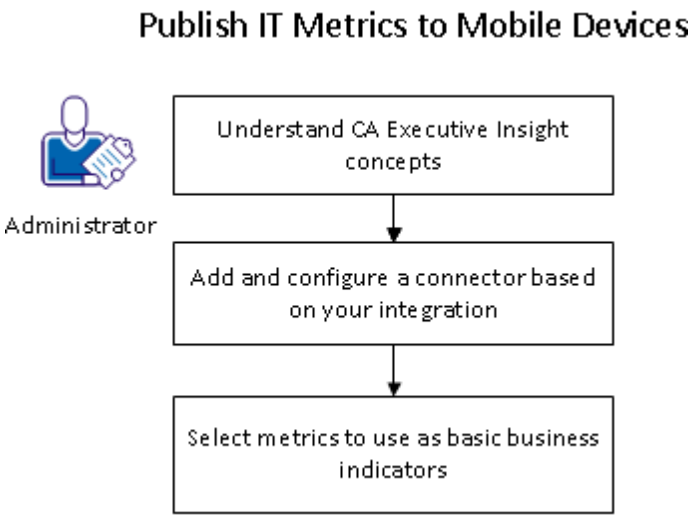
Chapter 6: Publish IT Metrics to Mobile Devices

This section contains the following topics:

Publish IT Metrics to Mobile Devices

As an administrator, you are responsible for configuring metric connectors and building business indicators for your users.

The following illustration describes how an administrator publishes IT metrics to mobile devices using CA Executive Insight.



To publish IT metrics from CA APM, CA SOI, and CSV files to mobile devices, follow these steps:

1. Understand CA Executive Insight concepts (see page 56).
2. Add and configure a connector:
   a. Configure connector for CA APM (see page 59).
   b. Configure connector for CA Service Operations Insight (CA SOI) (see page 61).
   c. Configure connector for CSV files (see page 62).
   d. Configure connector for CA Capacity Command Center (CCC) (see page 67)
   e. Configure Web Service connector (see page 74)
3. Select metrics to use as basic business indicators (see page 76).

After you add the specific connector and select the metrics to use for basic business indicators, the connector starts polling for data.

Understand CA Executive Insight Concepts

Before you use CA Executive Insight to set up and view important IT metrics on your mobile device, it is important to understand some basic concepts.

To understand the basic concepts, read the following information:

- Business Indicators (see page 56)
- Categories (see page 57)
- Business Services (see page 58)
- Dashboards (see page 58)
- Metric Connectors (see page 59)

Business Indicators

Business indicators represent performance indicators of interest to your organization. Based on IT metrics, business indicators measure the performance of critical business activity that is dependent on IT services.

Currently, CA Executive Insight supports *basic business indicators*. Basic business indicators are business measurements that are directly mapped to an IT metric. You create basic business indicators that are based on the available metrics from different data sources in your environment such as CA APM.

The following scenarios illustrate the use of business indicators:

A line-of-business manager responsible for the launch of a critical new application requires a dashboard with a small set of metrics. The metrics roll up to top-level business indicators that measure the following:

- Daily, hourly, and weekly number of hits on the application
- Quality of the end-user experience
- Total revenue that is generated from the application
- Health of IT systems

An IT manager responsible for updating a sales and booking application requires a dashboard of business indicators to align IT to clear business objectives. The dashboard includes business indicators that measure the following:

- Health of the application
- Number of users currently logged in
- Number of dropouts
- Number of dropouts per day for one month
- Number of customers that completed a booking during the previous hour
- Average amount of time that is spent on each booking
- Availability of the booking application

Categories

Categories let you organize business indicators into groups that have meaning to your business. When you assign business indicators to a category, the business indicators are displayed in a dashboard that is automatically generated for that category. A business indicator can be assigned to multiple categories.

You create categories and assign business indicators to them based on the needs of the business and your users. For example, to support the executive responsible for a critical new application, you could assign the relevant business indicators to a category named CriticalApp. After logging in to CA Executive Insight, the executive can view the CriticalApp dashboard for the current values and trends.

Business Services

CA Executive Insight creates business services when new business indicators are created for supported metrics of any business service available in CA SOI. The product periodically synchronizes with CA SOI to maintain the same hierarchy of services as in CA SOI.

You cannot assign business indicators to a business service. Business indicators for a service are displayed in a dashboard that is automatically generated for that business service.

Dashboards

A *dashboard* provides a visual overview of business indicators that have been grouped for a specific purpose. For example, business indicators can be grouped to show the following values in a dashboard:

- Daily performance measurements for a specific line-of-business
- Real-time health of critical servers
- Customer experience of each geographic business segment

To create a dashboard, you assign the business indicators that you want to display in the dashboard to a category. For each category and business service created in the CA Executive Insight application, the application generates an on-the-fly dashboard of the business indicators that are assigned to that category.

From a dashboard, users can drill down into the details of a business indicator and can do the following:

- View the current, high, low, and average value of the business indicator
- Compare the current value of the business indicator with its previous value based on absolute value or percentage
- Know how long an SOI service metric has been in a particular state
- Identify trends that are based on historical information over different time periods
- Access annotations created by other users and add their own annotations
- Access historical data to know the average number of users that were recorded as logged in per hour over the course of one week

Metric Connectors

A *metric connector* creates a connection between a data source and the CA Executive Insight application. After the connection is established, the application retrieves IT metrics from the data source and publishes the metric data as business indicators in a dashboard.

CA Executive Insight supports such data sources as CA APM, CA SOI, and CSV files. To retrieve data, you add a connector and specify the connection information for the instance.

To retrieve metric data from multiple instances, you add multiple connectors.

To retrieve data for basic business indicators, a connector supporting the *poll interface* polls the current values of the selected IT metrics from the instance. In the case of connectors supporting the *push interface*, like the CSV Connector, the indicator data gets pushed when CSV files are uploaded against the connector.

Configure Connector for CA APM

To retrieve IT metrics from a CA APM instance, you add an CA APM connector. You can retrieve metric data from multiple CA APM instances by adding multiple CA APM connectors.

Important! To understand your dashboard data, the following polling values are important. For CA Introscope®, the selected metrics are polled once a *minute*. For CA CEM, the selected metrics are polled once an *hour*.

Follow these steps:

1. Log in to the Desktop UI.
2. Click Metric Connectors under the Admin tab.

   The Metric Connector page opens.
3. Click Add New, and select CA APM Connector from the drop-down list.

   The New CA APM Connector page opens.
4. Complete the following fields:

   Name

   Defines the name of the connector.

   Limits: Up to 255 characters.

   Note: The connector name is used internally and does not need to match any value on the CA APM instance.

Description

(Optional) Defines a description for the connector.

Limits: Up to 512 characters.

Protocol

Indicates a connection protocol. HTTP is supported.

Host

Specifies the fully qualified domain name or IP address or host name of the CA APM instance.

- For CA APM and CA Introscope®, specify the IP address or host name of the Enterprise Manager in a standalone environment or the MOM Enterprise Manager in a clustered environment.
- For CA CEM, specify the IP address or host name of the Customer Experience Manager TESS component.

Port

Specifies the port that the CA APM instance uses to communicate with the connector.

Limits: 0-65365

Notes:

- For CA APM and CA Introscope®, specify the web server port of the Enterprise Manager. The default CA APM web server port is 8081. This port is different from the Enterprise Manager port (5001) to which the Introscope Workstation and agents connect.
- For CA CEM, specify the port for the Customer Experience Manager TESS component. The default port is 80.
- To identify the port, check the IntroscopeEnterpriseManager.properties file, which is located in the config subdirectory of your CA APM or CA Introscope® installation.

Username

Specifies a user ID on the CA APM instance. Specify the administrator user or a user with privileges to invoke the Introscope and Customer Experience Manager web services.

Password

(Optional) Specified the password that corresponds to the Username value.

5. Click Save.

   CA Executive Insight tests the connection. If a connection cannot be established, an alert is displayed.

   After the connection is verified, the Metrics tab lists the metrics available for the CA APM instance.

Configure Connector for CA Service Operations Insight

CA Executive Insight lets you view your vital company business metrics on mobile devices. Business metrics can come from multiple sources including CA Service Operations Insight (CA SOI). This application displays selected CA SOI service models and the metrics available for each service. These metrics include: Health, Quality, Risk, and Severity. The product automatically displays the CA SOI services in a hierarchy, so you can simply select the important metrics to display on your mobile device.

The CA SOI poller fetches this information by invoking a web service available in CA SOI. The product will store and aggregate data from CA SOI service metrics and make them viewable on mobile devices as business indicators.

Important! To understand your dashboard data, the following polling values are important. For CA SOI, the selected metrics are polled once per minute.

Follow these steps:

1. Click Metric Connectors under the Admin tab.
2. Click Add New, and select CA SOI Connector from the drop-down list.

   Note: If CA SOI is installed on different machines as a UI and SA Manager, use the SA Manager server name/IP and port for creating the connector. The default port for CA SOI is 7090.

3. Click Save.

   The connector is usually created in about 1 minute. However, if you have numerous client installations in CA SOI server configurations, this time may be 10-15 minutes.

   You have created the connector.

4. Select the CA SOI service metrics that you want included.

   You can add business indicators from CA SOI connectors the same way you would for an APM connector, by selecting the service from the list. The product supplies a business indicator name for your service; however, you can click Update to further refine the name to your organizational needs. After an indicator is created against a CA SOI service metric, CA Executive Insight automatically creates a grouping for the business service in the same service hierarchy as in CA SOI. This hierarchy can be visualized in the mobile user interface under 'Business Service' in the 'Indicators' tab. The newly created business indicator will appear under this service.

Note: CA Executive Insight does a periodic synchronization with CA SOI to keep the service hierarchy synchronized with CA SOI. Changes automatically are visible in the desktop and mobile user interfaces. However, an Administrator can always force a re-synchronization with CA SOI by selecting the 'Save' button on the 'Connector Details' tab. This is helpful if a periodic synchronization has not completed successfully.

Important! To view these changes on your mobile device, refresh your mobile application.

Important! To maintain optimization, CA Executive Insight is stopped if not able to fully synchronize with CA SOI server more than five times, as this is very resource intensive. If all five attempts fail, the log displays an error message and the administration user interface displays the connector state as 'synchronization-failed' state. Manually save the connector to re-start a synchronization. A reboot is not required.

Configure Connector for CSV Files

CA Executive Insight enables you to view your vital company business metrics on mobile devices. These business metrics can come from many different sources including CSV (comma-separated values) files, which store tabular data in plain-text form. CA Executive Insight supports the following delimiters: comma, semicolon, colon, and tab.

CA Executive Insight lets you upload CSV file data into the CA Executive Insight database. This data can be made available on your mobile device.

Follow these steps:

1. Obtain or create one or more CSV files containing data that you want to view using the product.

   CSV files must have a row of timestamps and a column of metric names or vice versa. Optionally, the CSV files can also have a metric path or a unit of measure with each metric name. The units of measure, path, or both must be in separate rows or columns, but their orientation must be the same as the orientation of the metric names.

   Note: The maximum file size recommended is 2 MB for the CSV file. However this is a configurable value and you can update if needed.

Important! Increasing the file size can cause the server process to run out of memory, depending on the other load the server is processing. There is also the possibility of losing data if the persistence of data is not fast enough. Caution should be exercised before changing this value!

   You can update this property in:

   Windows

   `install_dir\config\execConfig.properties`

   Linux

   `install_dir/config/execConfig.properties`

   You can update this property by editing value:

   `service.dirMonitor.maxCsvFileSize=<desired file size in Megabytes>`

2. Click Metric Connectors under the Admin tab.

   The Metric Connector page lists connectors.

3. Click Add New, and select CSV Connector from the drop-down list.

4. Fill in the required fields (indicated with an *). Mouseover each field for a field description.

   Name

   Defines the name of the connector.

   Limits: Up to 255 characters

   A connector name is used as a folder name for the default location of CA Executive Insight; therefore, usage of special symbols such as ?, %, #, ;, |, <, >, \, / cannot be used in connector name.

   Note: The connector name should be unique.

   Description

   (Optional) Defines a description for the connector.

   Limits: Up to 512 characters

Folder Location

The default folder location is:
`<Executive Insight installation directory>/csvUploads/<connector name>`

Optionally, you can specify a folder location. To specify a different folder location, you can utilize a folder on a local or a remote machine. The folder should already exist as CA Executive Insight will not create the folder and will display an error message if the folder does not exist.

Specify the full path to access this folder. Shared folders on remote machines should be read-write share. Read-only share causes an error. If the product is not able to access the folders at a non-default location, an error message is logged in the log file. When the folder becomes accessible/reachable, the product resumes monitoring.

Delimiter

Select the delimiter of the CSV file from a drop-down list with four options: comma, semicolon, colon, or tab.

Default: Comma

Data Start Row #

Enter the required row number where the data begins in the CSV file. Supports numbers from 1 onward.

Data Start Column #

Enter the required column number where the data begins in the CSV file. Supports letters and numbers similar to the convention used by Excel.

In the files being used, there should be no non-numeric values after the Data Start Row and Data Start Column values.

Data Organization

Select the orientation of the data in the CSV file from a drop-down list.

- **Time is listed by column** - indicates that each column represents the data in a single time stamp for each metric in the CSV file.
- **Time is listed by row** - indicates that each row represents the data in a single time stamp.

Time Stamp Row/Column #, Metric Name Row/Column #, Metric Path Row/Column #

These fields represent which row/column each of those fields can be found.

Unit of Measure Row/Column #

It is not a required field. It can be specified in the uploaded file. It will be considered only when a business indicator is created. It is not updated in subsequent uploads when business indicator values are updated or ignored. To update this value for an already created business indicator, use the Admin User Interface or Business Indicator update page.

If this value is no longer supported by CA Executive Insight, it ignores and a log file message for this action is written.

Date/Time Format

Multiple date/time formats are selectable using a drop-down list, but you can also specify any formats unique to your organization. This format cannot contain the selected delimiter.

Note: In the files being used, there should be no non-numeric values after the Data Start Row and Data Start Column values. All the following values should be metric data.

5. Click Save.

   All properties for a connector can be updated and used for the next file that is processed. The CSV connector is created.

6. Place your CSV file(s) within the default folder or the folder location you specified.

   CA Executive Insight scans the designated folder location every minute and extracts data from all CSV files found in that directory, and creates or updates the appropriate business indicators. Only CSV file types are processed (with '.csv' extension); all other file types/extensions are ignored. For each CSV file, if the extraction is a success, the file is deleted from the source directory. If the extraction fails, a '.bad' extension is appended to the filename and the file remains in the monitored directory. CA Executive Insight outputs any error messages from the file extraction/upload to the log file.

   A business indicator is uniquely identified by metric name and metric path data.

   CA Executive Insight saves data at a per minute granularity. No more than 1 data value per minute is saved. If there is more than 1 data value for a minute, the 1st value, with respect to time stamp, is saved. All other values are ignored.

   The data is aggregated every hour on the half hour, such as 12:30, 1:30, and so on. No data will be available for timeframes other than 15M (15 minutes) or 1H (1 hour) until aggregation runs. Any data that is older than 1 hour will be displayed after the data has been aggregated. For some files, 2 aggregation cycles may be needed.

   If you upload a new file with data for existing business indicators for timestamps already in the database, updated values are used and aggregation are run again.

Date/Time Format Considerations

The date and time formats are not case-sensitive. The letter 'm' is context-sensitive based on whether 'h' or 's' is detected. If hour is detected, then next 'm' value will be minutes; or if seconds are detected, directly after the 'm' instances; otherwise, 'm' will indicate months.

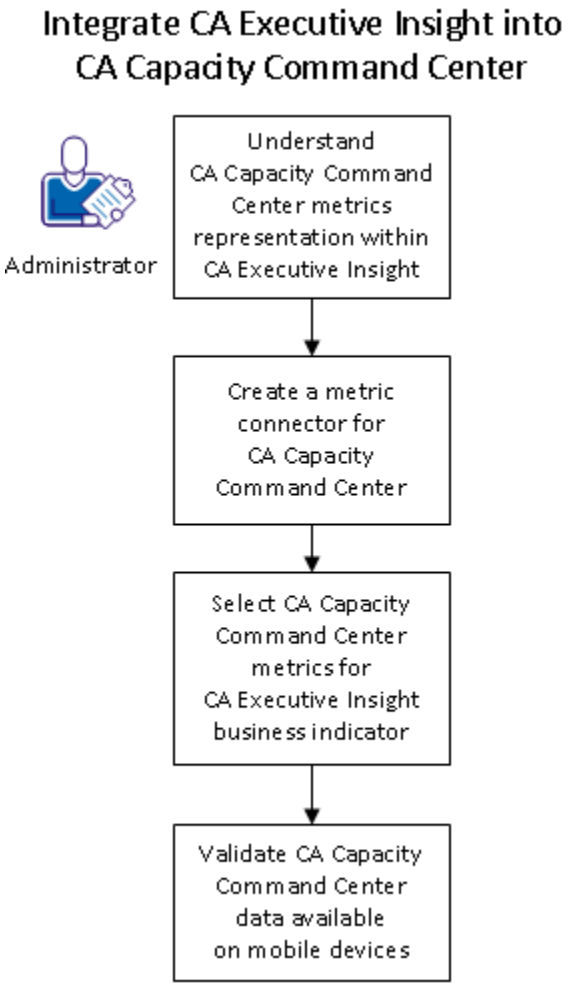
To Display	Use this format code
Months as 1 - 12	m
Months as 01 - 12	mm
Months Jan - Dec	mmm
Months as January - December	mmmm
Days as 1 - 31	d
Days as 01 - 31	dd
Days as Sun - Sat	ddd
Days as Saturday - Sunday	dddd
Years as 00 - 99	yy
Years as 1900 - 9999	yyyy
Hours as 0 - 23	h
Hours as 00 - 23	hh
Minutes as 0 - 59	m
Minutes as 00 - 59	mm
Seconds as 0 - 59	s
Seconds as 00 - 59	ss
Hours as 4 AM	h AM/PM

Configure Connector for CA Capacity Command Center

CA Executive Insight enables IT to quickly and easily provide real-time access to high-value metrics that measure the pulse of business. Designed specifically for the mobile platform and with the active user in mind, CA Executive Insight connects executives and decision-makers to real-time views of how the health and performance of key IT services impact business outcome.

CA Capacity Command Center is a comprehensive suite of capabilities that lets you maximize your efficient use of data centers so that you can guarantee performance and availability of their business services. The product simplifies the ongoing process of managing the capacity of your infrastructure.

The following illustration describes how an administrator integrates CA Executive Insight and CA Capacity Command Center.



Follow these steps to integrate CA Executive Insight with CA Capacity Command Center:

1. Understand CA Capacity Command Center metrics representation within CA Executive Insight (see page 70).
2. Create a metric connector for CA Capacity Command Center (see page 70).
3. Select CA Capacity Command Center metrics for CA Executive Insight business indicator (see page 70).
4. Validate CA Capacity Command Center data available on mobile devices (see page 71).

Understand CA Capacity Command Center metrics representation within CA Executive Insight

The CA Capacity Command Center metrics data selected for viewing on mobile devices is converted into CA Executive Insight business indicators and aggregated hourly and daily before they can be viewed.

Currently, CA Executive Insight represents two metrics of the CA Capacity Command Center's Efficiency category:

RxEfficiencyScore

This is presented as EfficiencyScore within CA Executive Insight.

RxEfficiencyScoreByOptimizationCategory

The Under value is presented as EfficiencyUnderUtilized within CA Executive Insight. The Over value is presented as EfficiencyOverUtilized within CA Executive Insight.

The same metric name within CA Capacity Command Center is used for many different groups; therefore, CA Capacity Command Center prefixes the metric names by the parent group name to make them unique when represented in CA Executive Insight.

The CA Executive Insight server polls the CA Capacity Command Center metrics daily by default starting at 30 minutes past midnight. If the CA Capacity Command Center server or data is unavailable, CA Executive Insight retries polling every two hours until data is returned or the start of the next periodic interval poll cycle. CA Executive Insight requests the data hourly. Ideally, 24 data points would be returned (for each hour in the past day). However, if the CA Capacity Command Center server is unavailable or has not finished its daily data calculations by the polling time, fewer data points could be provided. Also, it is possible that the CA Capacity Command Center pre-calculation rollup process has not been run for several days. To compensate, CA Executive Insight polls data for several preceding days and fills in the missing data from the previous poll or updates data if previously polled. For the number of the preceding days to perform polling (Late Data Range), see the section, Create a Metric Connector for CA Capacity Command Center.

Important! CA Capacity Command Center based business indicators may show no data for a requested data interval, if CA Capacity Command Center data has not been polled or aggregated by the CA Executive Insight server. Polling by CA Executive Insight results in no data if the precalculation rollup process has not been run on the CA Capacity Command Center server for the latest three days of CA Capacity Command Center data.

Create a Metric Connector for CA Capacity Command Center

Perform the following steps to create a metric connector for CA Capacity Command Center.

Follow these steps:

1. Log into the CA Executive Insight Admin tool.
2. Click the Metric Connector tab.
3. Select 'CCC Connector' from the Add New Tab list.
4. Fill in the fields and click Save.

   A new CA Capacity Command Center metric connector is created and the connector metrics form is displayed.

Select CA Capacity Command Center Metrics for CA Executive Insight Business Indicator

Select CA Capacity Command Center metrics using the Metric form. The form appears automatically after a new CA Capacity Command Center connector is created. You can also navigate to it by selecting a CA Capacity Command Center connector from the Metrics Connector screen.

Follow these steps:

1. Expand the folders on the form starting from the Root folder, to view and select the CA Capacity Command Center metrics.

   The metrics already selected for CA Executive Insight business indicators have a check mark in a status box.

   Green Status

   Indicates that the metric has data available.

   Orange Status

   Indicates that the metric has no data available for at least last three days.
2. Select a CA Capacity Command Center metric for CA Executive Insight use. You can select multiple metrics. Metrics that are not saved are noted by an asterisk.

3. Click Save.

After a metric is saved as a business indicator, its data becomes available for polling and aggregation by CA Executive Insight.

The business indicator inherits all of the functionalities of a CA Executive Insight business indicator, like the ability to have associated image, status thresholds, and unit of measure.

Use the business indicator form to update a business indicator.

Validate CA Capacity Command Center Data Available for Mobile Devices

Perform the following tasks to validate and view CA Capacity Command Center data on your mobile device.

Note: CA Capacity Command Center data becomes available for viewing only after being polled and aggregated by CA Executive Insight.

Follow these steps:

1. View the CA Capacity Command Center data on your desktop by calling the CA Executive Insight application using an applicable browser.
2. Select the dashboard mode to view multiple business indicators representing the CA Capacity Command Center metrics data values at the same time.
3. Select an individual business indicator to view a detailed view of a single CA Capacity Command Center data metric as a CA Executive Insight business indicator.

   You can specify alternate time views such as daily, monthly, and quarterly. By default the CA Capacity Command Center based business indicators will be presented for 1 month period.

   If a business indicator view is a graph, click within the graph to see a value at a specific time point.

Using Web Connectors

The Web connector feature lets you access data from remote web services for display in the mobile application dashboard. Any web service with Basic, Digest, or no authentication and responses in XML, JSON, or ATOM format is supported, for example, CA APM Cloud Monitor.

The Web connector feature supports:

- Authentication types: Basic, Digest, or none
- Response formats: XML, JSON, ATOM
- Metric and metadata request types
- Parameters for filtering data from web services
- The GET HTTP execution method
- Variables to pass data from one request to another

About Metric and Metadata Requests

Request Type	What You Should Know
Metric	■ Exposes available metrics and is visible in the Metric tab. ■ Use parameters to specify the data to collect from the web service. For example, you can use parameters to define time intervals (start and end).
Metadata	Executed on connector startup and every 12 hours by default. The default refresh interval can be modified by updating: http.connector.incrementalSync.reschedule FullSync.minutes in the file, INSTALL DIR/config/execConfig.properties ■ Not visible in the Metric tab ■ Output variables from executing this request can be used as inputs when configuring other requests.

About Variables

A common example of using variables is where one web service call is an authentication request that returns a “sessionId,” and a second web service call uses this “sessionId” as one of the inputs to get metric data. In this case, you must configure the first request as type “metadata” (which produces the variable sessionId), and the second is a “metric” request that consumes this variable as ${sessionId} to get the metric data.

Other notes:

- Variables are consumed in requests by specifying the variable name within ${}, for example, ${varname}
- If your request requires a time interval, use the named variables: $startTime{time format} and $endTime{time format}, where the time format is specified as a Java time format.
- Use curly brackets {} to specify a variable value for direct substitution. For example, to display stock quote, create a variable, Key = STOCK and Value = {CA}

Configure Web Services Connectors

The following steps show how to configure a Web Services connector to get metric and metadata that returns the response in XML format. The steps for processing JSON responses are similar; use JSONPath expressions to parse responses.

Important! A connector can contain more than one request, however multiple requests should be added to the same connector only if they have an interdependency. If a single request fails to execute, the connector enters a 'Failed' state' will not execute other requests until all requests can execute successfully.

1. In the Administrator user interface, go to: Metric Connectors and click Add New, Web Connector.
2. In the properties tab, enter information using the following entries as an example for collecting CA stock quotes:
   - Name: CA Stock
   - Request Name: CA Stock Quote
   - Method: GET
   - URL: http://finance.xyz.com/webservices/stockquote
   - Parameters: Key = stock, Value = CA
   - Authentication: None

   a. In the Response option button, select Status.

   b. Click the Test button, and verify that the Response status is: HTTP/1.1 200 OK.

   c. Change the Response option button to: Body, and verify that XML data is displayed.
3. To configure metric requests, click the Processing tab, and from the Type drop-down list, select Metric.

   a. In the Response option button, select Result.

   b. In the Metric Name field, enter the XPath expression to parse the metric name from the XML body, or constant values using curly brackets {}. The Xpath expressions must result in a NodeSet. Multiple expressions and or constant values must be separate by semicolon (;). For Node-Set-Function syntax, see the W3C XML Path Language (XPath) documentation.

   Example of an XPath expression: //field[@[name='name']

   Example of a constant value: {CAStock}

   Example of multiple expressions and constant values, which results in three metric names selected: //resource[2]/field[@name='name'];{CAStock};//resource[25]/field[@name='name']

c. In the Metric Value field, enter the XPath expression to parse the metric value from the XML body. The Xpath expressions must result in a NodeSet. Multiple expressions must be separate by semicolon (;).

   Example: //field[@name='price']

d. In the Metric Timestamp field, enter the XPath expression to parse the timestamp from the XML body. The Xpath expressions must result in a NodeSet. Multiple expressions must be separate by semicolon (;).

   Example: //field[@name='ts']

e. Select the Date/Time format. Use the examples in the drop-down list to match the timestamps in the response body.

   Note: If you do not specify a Timestamp expression or format, then the polling time is used as the timestamp of the indicator data.

   Note: Use Refresh Minutes to specify the frequency for polling data from the web service. This value cannot be updated after Business Indicators are created for a request.

   Note: If this request produces variables, they can be configured as an XPath expression to parse the variable value from the XML body, or constant values using curly brackets {}. The Xpath expressions must result in a NodeSet. Multiple expressions and or constant values must be separate by semicolon (;).

f. Click the Test button, and verify the processing results.

4. To configure metadata requests, click the Processing tab and from the Type drop-down list select Metadata.
5. Add one or more variables as an XPath expression to parse the variable value from the XML body, or constant values using curly brackets {}. The Xpath expressions must result in a NodeSet. Multiple expressions and or constant values must be separate by semicolon (;).
6. Click the Test button, and verify the processing results.

   A single connector can have multiple requests associated with it. Use ‘New’ to create additional requests. Use ‘Clone’ to make a copy of the existing request and make changes as needed. Any changes from ‘New’, ‘Clone’ or ‘Delete’ operations are not final until you click the 'Save" button to save the connector configuration.
7. After all requests are created, click Save and view the metrics in the Metrics tab.

Select Metrics for Business Indicators

For CA APM, CA SOI, CA CCC, and Web Service connectors, after you add the connector you want, select the metrics to use for basic business indicators. To retrieve data for basic business indicators, a metric connector polls the current values of the selected metrics from the data source.

Note: Selecting metrics does not apply to CSV files.

Follow these steps:

1. Select the metrics that you want to use for business indicators. To select a metric, navigate to the metric in the tree view and select the check box next to the metric.

   A business indicator is created for each metric you select. By default, the name of a business indicator is set to the name of its corresponding <metric parent path name>-<metric name>. Only the first 20 characters of the metric parent path name are utilized by CA Executive Insight.

2. (Optional) Edit the default names of the business indicators. To edit the default name of a business indicator, double-click the name in the Business Indicator Name column and specify an updated name.

3. Click Save.

   The Status column indicates whether a selected metric is active or unavailable. If a selected metric is active, the connector starts polling data for the corresponding business indicator.

   To get more information about a business indicator, mouseover the name in the Business Indicator Name column.

4. (Optional) You can assign categories or perform other supported bulk edit operations on all newly created Business Indicators using the 'Edit new indicator settings' link displayed with success/failure message.

Aggregation Considerations

CA Executive Insight runs a periodic aggregation process to aggregate the raw indicator data into lesser granular intervals. This facilitates visualization of aggregated data for the longer time ranges. It also helps minimize the amount of raw data that is retained in the database. The raw indicator data, which is typically one-minute interval data, is used to serve the 15 minute and the 1 Hour duration charts.

One part of the aggregation process runs hourly, which aggregates the raw interval data into hourly intervals. Therefore, this aggregates all raw data for an hour into one data point per hour per indicator. This data is used for visualizing the charts for the daily and weekly time ranges. This part runs 30 minutes past the hour, every hour. This running frequency ensures that there is enough time for gathering any late arriving interval data before aggregation begins.

The second part of the aggregation process runs daily, which aggregates the hourly interval data into daily intervals. Therefore, this aggregates all hourly data for a day into one data point per day per indicator. This data is used for visualizing the charts for the monthly, quarterly, and yearly time ranges. This will typically run as part of the aggregation that is kicked off after midnight. The daily aggregation process may also run right after an hourly aggregation if a previous daily aggregation process has not been completed normally.

The raw and aggregated data are purged daily based on the purge settings.

Chapter 7: Managing CA Executive Insight

This section contains the following topics:

Customize the Basic Business Indicators

After selecting metrics to use as basic business indicators, you can optionally customize the business indicators. For each business indicator, you can assign categories, specify a description, add custom branding, or change the business indicator name, visualization details, or measurement details.

Note: You cannot change the metric that the basic business indicator corresponds to.

Follow these steps:

1. Select Metric Connectors, Connector to select the connector.
2. On Metric tab, mouseover the row containing the basic business indicator you want to update.

   The Update link appears in the last column of the row.
3. Click Update.

   A page lists the details of the business indicator.
4. Update the information in the Information section as required:

   Name

   Defines the name of the business indicator.

   Limits: Up to 255 characters.

   Description

   (Optional) Defines a description for the business indicator.

   Limits: Up to 512 characters.

   ID

   The internal identifier for the business indicator.

Owner

Owner name that created the business indicator. Updates by a different user do not change the owner details. This is a read-only field, and cannot be modified.

Created/Modified

The machine time stamp when the business indicator was last created and/or modified. This is a read-only field, and cannot be modified.

5. Specify a Title Image to assign graphics to business indicators. A default logo library is available or you can specify your own meaningful graphics. The graphics must be PNG, JPG, or GIF file types. The minimum size is 50 pixels by 30 pixels. The maximum size is 800 pixels by 500 pixels.

   Note: A PNG-24 with transparent background is highly recommended.

   Click the 'Add Image' button to select a custom image for the business indicator.

6. Assign categories to the business indicator in the Organization section as required using the arrow icons. You can also drag and drop categories.

   Note: Before you can assign a business indicator to a category, you must create the category.

7. Update the information in the Measurement section as required:

   Type

   Indicates the type of business indicator.

   Source Name/Path/Connector

   Specifies the name, path, and connector of the source.

   If CA Executive Insight cannot verify the Source Path from the source connector, CA Executive Insight will display problem message(s) indicating 'Metrics not found for metric path: <metric path name>' or 'There is no measurement data for this Business indicator. There may be a problem with the source connector.'

   For an APM or CSV metric, you can edit the Source Path field to supply the correct path. For CSV, you should change the source path before the new data is uploaded to CA Executive Insight, so that the new source path in the CSV file can be validated. SOI will automatically update and the source path is then read only.

   Frequency

   Indicates the frequency of the polled value.

Calculation Type

Indicates the calculation type of the business indicator. Options are Average Aggregation and Sum Aggregation.

Note: Calculation Type is not available for Business Indicators from CA SOI data connector.

8. Update the information in the Visualization Type and Visualization Details sections as required:

Default Duration

The default time range that is used when a business indicator chart is drawn. The graph on the dashboard also displays the data based on the default duration. The duration is based on the connector type that the indicator belongs to. For example, 1M for CC BI, 1D for CEM BI, and 1H for all other BIs. The default duration can be changed from its default to one of the supported durations.

Units

Specify unit of measurement. Many default options are provided so you can easily select a unit of measurement. Some options include each, percent, currency (dollars, euros), data (bits, bytes, kilobytes), data rate (bits/second, megabits/second, gigabytes/second), time (milliseconds, minutes), time rate (/millisecond, /hour). You can also specify no units of measure or a custom unit of measurement specific to your organization.

Display Decimals

If unselected, real number values are rounded off to the nearest integer. If selected, values are display in decimal digits to a precision of two. For example, 983.575 is shown as 983.58. See the 'Status/Value - Status Thresholds' field description for details.

Visualization Type

Select from the available Visualization Type options, to determine the type of 'widget' to be used when the business indicator is displayed in a dashboard. Options are Line Chart, Status/Value, and Gauge.

Line Chart

CA Executive Insight automatically formats the line chart.

Status/Value - Status Thresholds

Selecting the Status/Value display options enable you to specify Status Thresholds. No Thresholds is the default, and then no further values are necessary.

If you select 'Larger values are good' then Threshold values appear enabling you to enter the Caution and Danger values that are meaningful for your organization. Then, the Good value is automatically all values *above* the Caution threshold value.

If you select 'Smaller values are good' then Threshold values appear enabling you to enter the Danger and Caution values that are meaningful for your organization. Then, the Good value is automatically all values *below* the Caution threshold value.

Gauge Display Settings

Specify the minimum and maximum values, and optional threshold settings, for the gauge widget. See the 'Status/Value - Status Thresholds' field description for further details.

Note: If you selected Calculation Type of Sum Aggregation, then the values entered here are per *minute*.

Note: The Visualization Type, Units, and Display Decimal Values are note available for Business Indicators from SOI data connector.

9. Click Save.

   The changes are saved.

10. Repeat the previous steps to update the remaining basic business indicators as required.

    CA Executive Insight publishes IT metrics as business indicators from the APM instance to a mobile device.

Update Multiple Business Indicators using Bulk Edit

You can update multiple business indicators to assign or un-assign categories or change the business indicator's measurement of visualization details.

Note: You cannot change the metric to which the basic business indicator corresponds.

Follow these steps:

1. Click Business Indicators under the Admin tab.

   The Business Indicators page lists the defined business indicators. The 'Max Per Page' field allows you to display many more business indicators by selecting values such as 15, 25, 50, 75, or 100.

2. Select multiple business indicators that you want to update by selecting multiple check boxes. Alternatively, you can select *all* business indicators that are displayed on your page by clicking the check box at the top of the list.

3. To delete business indicators, select the 'Delete' button at the top of the business indicator list. A confirmation message appears.

4. To edit business indicators, select the 'Edit' button at the top of the business indicator list.

   The Bulk Edit Business Indicators screen appears, enter values as described below.

   Select Save when complete. If there are no errors, the business indicators list view is displayed with a message confirming the changes have been saved. If there are errors, this page remains displayed until the error is resolved.

Selected Indicators

- The indicators are listed in two columns from left to right and vertically. Long indicator names maybe be truncated to fit within the column width.
- If you click the 'X' it removes the indicator from the list. When an indicator is removed, the Organization, Visualization Details, and Measurements sections are recalculated.
- Hovering on a selected indicator displays a tooltip to list categories.

  Note: If you remove selected indicators, then final selections on a Cancel action are not propagated back to the business indicators list.

Organization

- The available column displays a list of all categories available.
- You can move categories between the available and assigned columns by using the arrows.
- When displayed, the assigned column shows only categories that are common to *all* selected indicators. If individual categories have business indicators assigned, these should *not* be shown.
- The 'Remove and replace all currently assigned categories' field is unchecked by default. If all categories assigned are common for selected indicators, the checkbox area is disabled but present.
- If the 'Remove and replace all currently assigned categories' field is checked, then you will be alerted with a pop-up of removal and replacement of uncommon indicators. This requires your confirmation.

Title Image

- If settings are common across all selected indicators, the 'Preview' field displays the current image, or 'No Image'; otherwise 'Multiple Images' is displayed.

Measurement

- 'Calculation Type' is the only field that can be changed across indicators.

  Note: If SOI and non_SOI business indicators are selected, you cannot change the measurement settings. In this case, the section displays an appropriate message, such as 'Measurements have been disabled because the indicators selected do not share the same measurement settings.'

Visualization Details

- Depending on the type of indicators selected, one or more fields that are common across the indicators are displayed.
- Default Duration can be edited in bulk across all indicators. If only non-SOI indicators are selected then Units, Display Decimal Values and Visualization Type and its dependent fields can be edited in bulk.
- Making a change to any section highlights that area to indicate it has changed and needs to be saved.

See Customize the Basic Business Indicators (see page 79) section for additional information on business indicator updates.

Create a Category

You can create categories to organize business indicators into groups that have meaning to your business. After you create a category, you can assign business indicators to the category based on the needs of the business and your users. You can assign a business indicator to multiple categories.

Follow these steps:

1. Click Categories under the Admin tab.

   The Business Indicator Categories page lists the defined categories.

2. Click Add New and complete the following fields:

   Name

   Specifies the category name.

Description

(Optional) Specifies the category description.

Title Image

(Optional) Specify a Title Image to assign graphics to the categories. A default logo library is available or you can specify your own meaningful graphics. The graphics must be PNG, JPG, or GIF file types. The minimum size is 50 pixels by 30 pixels. The maximum size is 800 pixels by 500 pixels.

Note: A PNG-24 with transparent background is highly recommended.

Click the 'Add Image' button to select a custom image for the category.

3. Click Save.

The category is created. You can now assign business indicators to the category by updating the business indicators.

Chapter 8: Configuring CA Executive Insight

This section contains the following topics:

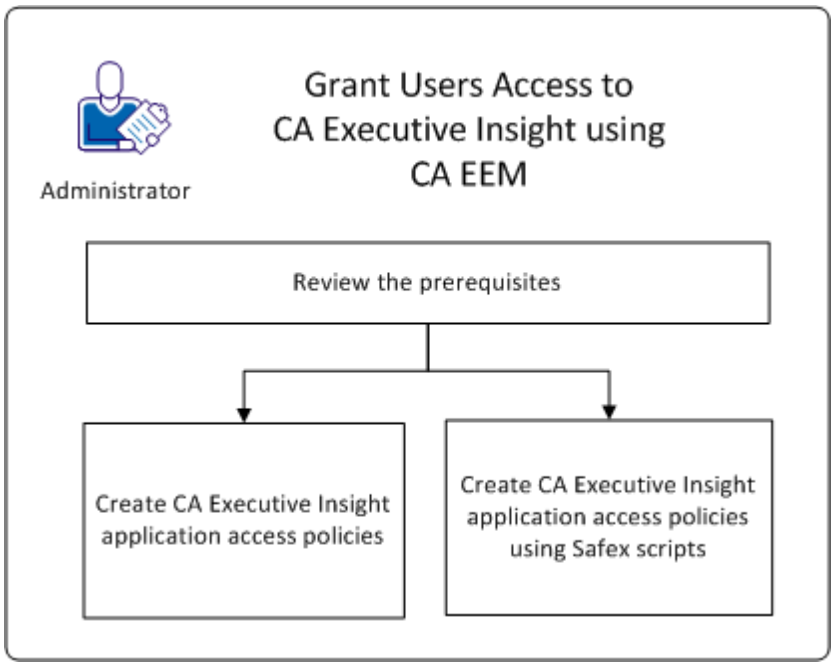
Grant Access to CA Executive Insight using CA EEM

CA Executive Insight uses CA Embedded Entitlements Manager (CA EEM) so that administrators can use role security to do the following tasks:

- Control access to the Administration user interface
- Control access to Business Indicators belonging to specific Categories and Business Services

CA EEM provides a common web interface, and the ability to use XML scripts to define policies, manage users, and audit user activities. CA Executive Insight uses CA EEM as a single source to authenticate users and manage user access rights.

The following illustration describes how to grant access to the product using CA EEM.



To grant access to CA Executive Insight using CA EEM, follow these steps:

1. Review the prerequisites (see page 88).
2. Create the access policies:
   a. Create CA Executive Insight application access policies (see page 89).
   b. Create CA Executive Insight application access policies using Safex Scripts (see page 92).

Review the Prerequisites

Before you create a user, verify the following:

- CA EEM is already installed and configured
- CA EEM administration credentials are appropriately established for yourself

Note: For additional information, see the CA Support page and reference the 'CA Embedded Entitlements Manager' documentation set.

During CA Executive Insight installation, the CA EEM application 'ExecutiveInsightforSA' name is created, or updated during re-install.

Note: 'ExecutiveInsightforSA' is the default name for CA EEM application. You may have updated this application name during the CA Executive Insight installation, in which case, use the name you specified.

The 'ExecutiveInsightforSA' file contains three resource classes and corresponding default access policies that were automatically created:

Resource Class	Access Level Description	Default policies Created
Administrator	Limit CA Executive Insight administration to selected users	Administration-All-Full Enables all users to have full permission.
Business Service	Limit viewing specific business service indicators to selected users	BusinessService-All-Read-All Enables all users to have read permission for all business services and indicators contained within those.
Category	Limit viewing specific category indicators to selected users	Category-All-Read-All Enables all users to have read permissions for all categories and indicators belonging to them.

To have a role-based security access, you need to modify or delete the default policies and create your own according to your product's installation security requirements.

Create CA Executive Insight Application Access Policies

You can create a user and can assign the user to various CA Executive Insight business services or categories.

Follow these steps:

1. Open CA EEM, select ExecutiveInsightForSA from the Application list, and log in as an Administrator.

   The CA EEM home page opens.

2. Click Manage Access Policies.

   The Policies page opens.

3. Click the Explicit Grants tab to view grant policies or the Explicit Deny tab to view deny policies.
4. Select an Access Policy class: Administration, BusinessServices, or Category to view/add/update/delete the corresponding policies.
5. Select the type of policy to create:

    For an explicit GRANT (the green color indicates allowing users privileges)

    For an explicit DENY (the red color indicates denying users privileges)

   The New Access Policy form opens.
6. Specify all General field values, such as Name, Type, etc.
7. Do the following in the Identities section:
   a. Select User or Group from the Type list.
   b. Click Search Identities button.

      The Search Identities fields display.
   c. Click Search.

      A list of Users or Groups displays.

      Note: This assumes you have preestablished users and groups defined in CA EEM. If not, you need to create them first.
   d. Select the users or user groups and use the arrow button to populate the 'Selected Identities' column.
   e. After you have specified the users, within the 'Add resource' field you enter the application resources, like BusinessService or Category name. You click the plus (+) button for every resource you add to the policy. You can leave the field blank if the policy applies to all resources.

   Note: In case the Business Service to be specified as a resource name in the policy is hierarchical, then provide the whole path leading up to the name. Delimit the different nodes in the path by using the colon character. See Business Service Specified as Resource Name Considerations below.

   Important! The name of the resource must exactly match as it is defined in CA Executive Insight.

   Note: The Administration class policies do not need a resource name.
8. Select an appropriate action(s), like Read or Full by using the action check-box.

9. The policy now provides (or denies for Explicit Deny policy type) the specified users access to the BusinessService or Category defined and also to the indicators belonging to the specific Category or Business Service or Administrative privileges (if the policy is tied to the Administration class).
10. Select 'Save'.

    The access policy is created.

Important! CA Executive Insight is not able to update CA EEM automatically when a new category or business service is added, deleted, or updated. Use CA EEM to create the corresponding access policies as needed.

Business Service Specified as Resource Name Considerations

If you specify the Business Service as a resource name and the policy is hierarchical, then provide the whole path leading up to the name. Delimit the different nodes in the path using a colon character. For example, the following Business Service name consists of three hierarchical nodes: Android-Service, Android-Main, and Android_DSN-2.
`Android-Service:Android-Main:Android-DNS-2`

In order to grant or deny access to the Android-Service:Android-Main:Android-DNS-2 service and its business indicators full path Android-Service:Android-Main:Android-DNS-2 has to be used as a resource name in the EEM Access Policy. Also, to be able to see lower level nodes on a mobile device while displaying Business Services in a hierarchical menus all the higher level nodes have to be also listed as Access Policy resource names. In the previous example this would be Android-Service and Android-Service:Android-Main.

Because listing all these resource names in Access Policies is resource intensive, the '*Treat resource names as regular expressions*' flag may be used. For example, a single resource name **'Android*'** and the flag turned on all will achieve the same result as listing all three full node names as resource names.

The above example assumes Business Service nodes hierarchical structure is reflected in the node names. If this is not a case, using a resource name as a regular expression still can make the Access Policy creation task easier. For example, for the following Business Services an access to a financial data is denied to a group of users.

```
NorthAmerica:FinancialService:CA
NorthAmerica:FinancialService:MA
NorthAmerica:FinancialService:NY
```

The explicit denial Access Policy for the user group with resource name, use the following example and a regular expression flag can be created to achieve the task.

```
^ NorthAmerica: FinancialService
```

Special Considerations for Business Indicator Authorization

A business indicators access authorization is performed based on its membership in a Category or a Business Service.

To be authorized a business Indicator must satisfy at least one of the following conditions:

- belong to at least one authorized Category
- belong to at least one authorized immediate level parent Business Service
- does not belong to any Category or Business Service

Note: If you are explicitly denied access to a Category or Business Service, it does not necessarily imply denial of access to all contained business indicators. If the same business indicator also belongs to other groups (either category or Business Service), one of which is explicitly granted access to the user, then the user will still be allowed access to this indicator.

Create CA Executive Insight Application Access Policies Using Safex Scripts

The safex script can be used to set access policies as well as the CA EEM Web Application. This is especially useful in the case of many policies. It can be more efficient instead of manually specifying each policy.

Below is a sample fragment of a CA EEM Safex Script:

```
<Policy name="Category-FinOfficers-Read-Financial" folder="/Policies">
<Description>EI Category policy - only FinOfficers group  users have read permission
for the Financial category </Description>
        <ResourceClassName>Category</ResourceClassName>
        <Identity>gug:finOfficers</Identity>
        <Action>read</Action>
        <Resource>Financial</Resource>
</Policy>
```

Note: For additional information, see the CA Support page and reference the 'CA Embedded Entitlements Manager' documentation set.

Modify the CA EEM Connection Properties

To change the CA EEM connection properties that are entered during installation, modify them manually by editing the EEM.properties file. This also allows you to change to a different CA EEM server or update the connection credentials if they change in the future.

Follow these steps:

1. Use a text editor to update the file:

   - On Windows:

     install_dir\config\EEM.properties

   - On Linux:

     install_dir/config/EEM.properties

   install_dir

   Specifies the directory where CA Executive Insight is installed.

2. Modify the following properties as appropriate:

   host

   Specifies the name of the server that hosts CA EEM.

   username

   Specifies the CA EEM administrator user name.

   Default: EiamAdmin

   password

   Specifies the password for the CA EEM administrator user. The password is encrypted.

   appname

   Specifies the CA EEM application name that is designated for CA Executive Insight.

   Default: ExecutiveInsightForSA.

3. Save the EEM.properties file.

4. Restart the CA Executive Insight server.

   The CA EEM connection properties are modified.

Modify the CA EEM Server Configuration

To configure a CA EEM after initial installation or modify the CA EEM server you are accessing, update the CA EEM server. Do this manually or use the Safex tool in the iTechnology directory to run the corresponding xml scripts. CA Executive Insight provides several sample scripts to use as templates in the following directory:

- Windows
  `Install_dir\security\EEM\sample.scripts`
- Linux
  `Install_dir/security/EEM/sample.scripts`

- To register CA Executive Insight application, use the following script:
  `eem.register.app.xml`

  This file also has samples for adding user groups, adding users to groups, and creating policies for role security feature.
- To unregister CA Executive Insight application, use the following script:
  `eem.unregister.app.xml`
- To add new CA Executive Insight users, use the following script:
  `eem.add.global.identities.xml`
- To remove CA Executive Insight users, use the following script:
  `eem.remove.global.identities.xml`

Change the Password for the Database Administrator User

If the password for the MySQL database administrator user is changed, configure the product manually to use the new password.

Follow these steps:

1. Generate an encrypted password for the database administrator user.
2. Use a text editor to open the following file:
   - On Windows:

     install_dir`\config\masterDbCredentials.properties`
   - On Linux:

     install_dir`/config/masterDbCredentials.properties`

   install_dir

   Specifies the directory where CA Executive Insight is installed.
3. Set the javax.persistence.jdbc.password property to the encrypted password you generated in Step 1.
4. Save the masterDbCredentials.properties file.

5. Enter the following commands using the MySQL client:

   ```
   use master;
   update tenant_dbconfig set password='encrypted_password' where id=n;
   ```

   encrypted_password

   Specifies the password (encrypted) for the database administrator user. Specify the encrypted password you generated in Step 1.

   n

   Specifies the tenant ID.

   Note: After installation, the tenant ID is 1. However, if you dropped and recreated the tenant database after installation, the tenant ID increments.

   The password is updated in the tenant_dbconfig table in the master schema.

6. Restart the CA Executive Insight server.

   The password for the database administrator user is changed.

Generate an Encrypted Password

If the password for the CA EEM or database administrator user changes, generate an encrypted password using the password utility that is provided with the product. After you generate the encrypted password, copy it into the corresponding property file and restart the server for the changes to take effect.

Follow these steps:

1. Change to the following directory at the command prompt:

   - On Windows

     ```
     install_dir\bin\
     ```

   - On Linux:

     ```
     install_dir/bin/
     ```

   install_dir

   Specifies the directory where CA Executive Insight is installed.

2. Enter the following command:

   - On Windows:

     ```
     EncryptPasswordTool.bat
     ```

   - On Linux:

     ```
     EncryptPasswordTool.sh
     ```

   You are prompted whether to mask the password input.

3. Specify whether to mask the password input by entering **y** or **n**.

   You are prompted to enter a password.

4. Enter your password.

   The utility responds with your encrypted password. You can copy the encrypted string into the corresponding property file.

   You are prompted whether to continue to use the utility.

5. Enter **y** to encrypt another password or **n** to end the utility.

Purging Data from the CA Executive Insight Database

Over time, the data in the CA Executive Insight database can become huge. To reduce the amount of data stored in the database, CA Executive Insight purges expired data from the database every day based on a specified retention criteria. For example, if the data retention criteria is 100, all data older than 100 days are deleted from the database. The data purge usually occurs daily, after midnight; however, it can also occur at the re-start of the CA Executive Insight server if the last purge process didn't complete successfully.

The retention criteria are stored in the CA Executive Insight database in the tenant_settings table as follows:

id	DisplayName	name	value
1	Biz Indicators Raw Data Retention days	rawDataRetentionDays	3
2	Biz Indicators Hourly Aggregated Data Retention days	hourlyDataRetentionDays	14
3	Biz Indicators Daily Aggregated Data Retention days	dailyDataRetentionDays	730

rawDataRetentionDays

Specifies the raw data retention criteria in days.

Default: 3

Limits: 1 or greater

hourlyDataRetentionDays

Specifies the hourly aggregated data retention criteria in days.

Default: 14

Limits: 7 or greater

dailyRetentionDays

Specifies the daily aggregated data retention criteria in days.

Default: 730

Limits: 90 or greater

To change the retention criteria, you can use an SQL update query. For example, the following query sets the daily aggregated data retention criteria to 100 days:

```
UPDATE tenant_settings SET value=100 WHERE  id=3;
```

For the change to take effect, you must restart the CA Executive Insight server. At server startup, the retention criteria values are validated. If a value is less than its minimum value, the default value is used and an error message is displayed in the CA Executive Insight server log.

Configuring CA Executive Insight Authentication Service

When you successfully log into the CA Executive Insight application using an Internet browser, a new authenticated session is created for you. The session data are passed to the browser (as a cookie) and used in the subsequent requests to identify the user without going through the full authentication process with the CA EEM server. However, for security reasons, the session validity has its limitation that can be configured as needed.

The session limitations are stored in the CA Executive Insight database in the tenant_settings table as follows:

id	DisplayName	name	value
6	Browser session automatic re-authentication minutes	sessionReAuthenticationMins	30
5	Browser inactive session expiration hours	sessionExpirationHours	24

sessionReAuthenticationMins

Specifies the re-authentication period in minutes. This is how long a user session is valid without a re-authentication with the CA EEM Server. When this period expires a user session is automatically re-authenticated with the CA EEM server. If the re-authentication fails, you need to re-login to CA Executive Insight.

Default: 30

Limits: Minimum 10, Maximum 180

sessionExpirationHours

Specifies the expiration period in hours. This is how long an inactive user session is valid without a user re-login. When this period expires, you will be prompted to re-login into CA Executive Insight.

Default: 24

Limits: Minimum 6, Maximum 72

To change the session authentication limits, you can use an SQL update query. For example, the following query sets Browser session automatic re-authentication minutes to 60.

```
UPDATE tenant_settings SET value=60 WHERE id=6;
```

For the change to take effect, you must restart the CA Executive Insight's server. At server startup, the session authentication limits are validated. If a value is less than its minimum value or greater than its maximum value, the default value is used and an error message is displayed in the CA Executive Insight server log.

Use HTTPS to Secure Communication

By default ,CA Executive Insight uses HTTP for all communications, including CA Executive Insight server to data source communication. You can configure CA Executive Insight to use HTTPS:

- Between the CA Executive Insight user interfaces and the server
- For the mobile application user interface component (for an internet accessible deployment)

This procedure describes how to configure SSL on CA Executive Insight version 1.1 with a self-signed Certificate and a certificate from a trusted SSL certificate provider.

The first step(s) should be to setup and verify that the Self Signed certificate functions. Once the self-signed certificate is configured and Tomcat is running on the SSL ports specified, you can follow the instructions provided by the Certificate Authority to put the official Certificate in place.

Configure SSL

Use the following steps to configure SSL for a self-signed certificate or trusted certificate provider:

1. To generate a self-signed certificate, from the command line, run the following command:
   `$JAVA_HOME\bin\keytool -genkey -alias tomcat -keyalg RSA -keystore keystore`

   On UNIX, make sure that the directory in which you generate the keystore file has appropriate permissions.

   Note: For more details about specifying a different keystore file location, see the Tomcat documentation.

2. Answer the prompts appropriately.

   Note: Both passwords should be the same.

   File 'keystore' is generated.

3. Copy the generated keystore file to the following directory:
   `Install_dir\config\`

4. Edit the server.xml file for your installation:

   For server installation, go to:
   Install_dir\product\ServerAndUI\plugins\catalina.start.osgi.config.fragment_1.0.0\ conf.

   For web UI installation, go to:
   Install_dir\product\WebUI\plugins\catalina.start.osgi.config.fragment_1.0.0\ conf

5. Edit the server.xml file located in the following directory:
   `Install_dir\product\ServerAndUI\plugins\catalina.start.osgi.config.fragment_1.0.0\ conf.`

a. Uncomment the following SSL connector:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
```

b. Modify value for 'keystorePass=' with password used in Step 2:

```
<Connector
 port="8443"
 scheme="https"
 secure="true"
 clientAuth="false"
 keystoreFile="${catalina.home}/config/keystore"
 keystorePass="<user defined password specified in keystore file>"
 sslProtocol="TLS"
 compression="2048"

compressableMimeType="text/html,text/xml,text/plain,text/javascript,text/
css"
 useSendfile="false"
 />
```

Note: If you want disable support for http comment the following connector '<!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->' section in the 'server.xml' file.

6. Restart CA Executive Insight.
7. To access the CA Executive Insight web interface with SSL, use: `https://hostname:8443/ or https://hostname:8443/admin/.`

   Note: You can specify a port other than 8443 in the server.xml file.

Once the SSL is up and functional with the self-signed certificate; you are ready to implement an official Certificate Authority provided certificate.

Configuring Official Certificate from Third Parties

Note: Each Certificate Authority should provide specific steps for their Certificate for Tomcat.

There will likely be additional steps past the above documentation, such as importing the certificate into the Install_dir\java\lib\security\cacerts file. These additional steps are beyond the scope of this documentation.

Follow these steps:

- Import the certificate received from the certificate authority:

  ```
  keytool -import -trustcacerts -file newcert.crt -file
  "Install_dir\config\keystore" -alias tomcat
  ```

  Note: Please review with your certificate authority if the self-signed certificate works but the official certificate authority provided certificate does not.

Disabling HTTP in CA Executive Insight

After SSL on CA Executive Insight is up and functional, you should disable HTTP.

Follow these steps:

1. Edit the server.xml file.

   For server installation, go to:
   Install_dir\product\ServerAndUI\plugins\catalina.start.osgi.config.fragment_1.0.0\conf

   For web UI installation, go to:
   Install_dir\product\WebUI\plugins\catalina.start.osgi.config.fragment_1.0.0\conf

2. Locate and comment the HTTP Connector section

```
<!--
<Connector
      port="8443"
      compression="2048"

compressableMimeType="text/html,text/xml,text/plain,text/javascript,text/css"
      useSendfile="false"
  />
   -->
```

3. Restart CA Executive Insight.

How to Change the Protocol or Port on the Executive Insight Server

If you change the protocol or port on the Executive Insight Server, update the configuration of the Mobile Application User Interface to ensure proper communications between the servers.

Follow these steps:

1. Go to: INSTALL_DIR/config/execWebUIConfig.properties and change the relevant properties.
2. Restart the mobile application user interface.