CA UIM Security v8.4

This document provides a summary of the security information in the existing CA UIM documentation. This information is provided as a reference and is not intended to override your own internal policies and security best practices.

Account Management

The Account Admin portlet allows bus users to manage account contact users and access control lists (ACLs) for user groups. You must have appropriate ACL permissions to view and make changes within the Account Admin portlet. For more information about account management, see Using Account Admin.

Types of Users

Two types of users exist in the CA Unified Infrastructure Management solution—*bus* users and *account contact* users. The permissions for both user types are set in the user's ACL. Administrators can create users of these two types as needed to meet their access control or multi-tenancy needs.

The following chart describes the key differences between bus users and account contact users.

Bus Users	Account Contact Users
Stored in the hub security file.	Stored in CM_ database tables.
Can see all data, systems, and alarms within UIM.	Can only see data, systems, and alarms with origins that match at least one of the account's origins.
Can access legacy Windows UIs.	Cannot access legacy Windows UIs.
Can access the bus, callbacks, and messages.	No bus access.

CA UIM User Password Policy

All passwords are installed in an encrypted format. The CA UIM server administrator account password must meet the following requirements:

- Be at least six characters
- Not exceed a maximum of 254 characters
- Cannot be the same as the username (For example, administrator)

We recommend that you configure your user accounts to follow your own internal policy.

UMP User Password Policy

All passwords are installed in an encrypted format. CA does not have a policy for UMP users. We recommend that you adhere to your organization’s internal policy for the creation of account passwords.

Database User Password Policy

CA does not have a policy for database users. We recommend that you adhere to your organization's internal policy for the creation of account passwords.

Logging of Failed Login Attempts

Admin Console

Set the log level on the service_host probe to level 4 or higher to have the system log failed login attempts. Log levels lower than 4 do not report when a failed login attempt occurs. Failed login attempts result in a log entry in service_host.log indicating a severe error. The following message is an example of a service_host.log entry for a failed login:

```
Dec 02 11:12:59:179 [tomcat, service_host] SEVERE: Login Error 2: Received
status (12) on response (in sendRcvLogin) for cmd = 'login'
```

UMP

Set the log level on the wasp probe to level 3 or higher to have the system log failed login attempts. Log levels lower than 3 do not report when a failed login attempt occurs. Failed login attempts result in a log entry in wasp.log. The following message is an example of a wasp.log entry for a failed login:

```
Dec 02 14:00:00:778 INFO  [http-bio-80-exec-7,
com.nimsoft.nimbus.probe.service.wasp.auth.LoginModule] Login failed: Wrong
username and/or password.
```

ACL Permissions List

Permission	Administrator	Guest	Operator	Superuser	Description
Accept	Y	-	Y	Y	Assign alarms to yourself.
Account Administration	Y	-	-	Y	Manage Account contacts and customize their portal content.
Acknowledge	Y	-	Y	Y	Close alarms.
Alarm Details	Y	Y	Y	Y	General access to alarm lists and alarm details
Alarm History	Y	-	Y	Y	Transaction history and alarm queries.
Alarm Management	Y	-	-	Y	Various alarm management features.
Alarm Summary	Y	Y	Y	Y	Display alarm summary information.
Archive Management	Y	-	-	Y	Create and modify packages.
Assign	Y	-	-	Y	Assign alarms to another user.
Automation - View Items	Y	-	Y	Y	Unimplemented.
Automation - Change configuration items	Y	-	Y	Y	Unimplemented.
Automation - Manage Workflows	Y	-	Y	Y	Unimplemented.
Automation - Create and Modify Workflows	Y	-	Y	Y	Unimplemented.

Basic Management	Y	-	-	Y	Manage (create, read, update, delete) the monitoring infrastructure.
Change Password	Y	-	Y	Y	Contact can change own password.
Cloud UE Monitor	Y	-	Y	Y	Access to Cloud User Experience Monitor portlet.
Custom Dashboards	Y	Y	Y	Y	Display custom dashboards.
Custom Reports	Y	Y	Y	Y	Display customer reports.
Dashboard Design	-	-	-	Y	Create, modify, and delete dashboards.
Dashboard Designer	Y	-	-	Y	Create, modify, and delete private dashboards.
Dashboard Download		-	-	Y	Download dashboards from archive.
Dashboard Upload	-	-	-	Y	Upload dashboards to archive.
Default Customization	Y	-	-	Y	Customize default portal content for bus users.
Discovery	-	-	-	Y	Discover and create template panels. **Note:** Only bus users with the Discovery Management permission in their ACL can perform discovery.
Discovery Management	-	-	-	Y	Set computer system properties.
Discovery Pie	-	-	-	Y	Display discovery information,
Distribution	Y	-	-	Y	Distribute archive packages.
Dynamic Views	Y	-	Y	Y	Display Dynamic Views.
Dynamic Views Dashboards	Y	-	Y	Y	Display Dynamic Views dashboards.
Dynamic Views Reports	Y	Y	Y	Y	Display Dynamic Views Reports.
Dynamic Views States	Y	-	Y	Y	General access to Dynamic Views alarm state information.
Edit Maintenance Mode Devices	Y	-	-	Y	General access to Dynamic Views alarm state information.
Edit Maintenance Mode Schedules	Y	-	-	Y	Create, edit and delete maintenance mode schedules.
Edit URL Actions	Y	-	Y	Y	General access to Dynamic Views alarm state information.
Execution Level1	Y	-	-	Y	Probe Command Execution Level 1.
Execution Level2	Y	-	-	Y	Probe Command Execution Level 2.
Execution Level3	Y	-	-	Y	Probe Command Execution Level 3.
Extended Security	Y	-	-	Y	Various security maintenance features.
Invisible Alarms	-	-	-	Y	Show alarms that are set to be invisible.
Launch URL Actions	Y	-	Y	Y	Launch URL actions associated with alarms.
License Management	Y	-	-	Y	Add and delete licenses.

List Designer	Y	-	-	Y	Create, modify, and delete lists and groups.
List Viewer	Y	-	Y	Y	View lists and groups.
Maintenance Mode	Y	-	-	Y	Robot maintenance mode management.
Manage ACL	Y	-	-	Y	Create, modify, and delete ACLs.
Manage Profiles	Y	-	-	Y	Create, rename, and delete user profiles.
Management Tools	Y	-	-	Y	Various tools (find/connect, etc.).
Modify Profiles	Y	-	-	Y	Modify and save user profiles.
NetFlow	Y	-	Y	Y	Access to NetFlow portlet.
NetFlow Configuration	Y	-	Y	Y	Allow portlet users to configure NetFlow probe settings.
NFA Manage Reports	Y	-	-	Y	Create, modify, delete, and execute reports.
NFA Run Reports	Y	-	Y	Y	View and execute defined reports.
NFA View Conversations	Y	-	Y	Y	Allow users to see specific client conversations.
NFA View Hosts	Y	-	Y	Y	Allow users to see specific client host conversations.
NFA View Protocols	Y	-	Y	Y	Allow users to see protocol information.
NFA View ToS	Y	-	Y	Y	Allow users to see the Type of Service information in applicable views.
Portal Administration	Y	-	-	Y	Web portal admin access.
Probe Basic	Y	-	Y	Y	Read-only view of the probe configuration.
Probe Configuration	Y	-	-	Y	Probe configuration tool management.
Probe Security	Y	-	-	Y	Manage probe security settings.
Program Options	Y	-	-	Y	Change various program attributes.
QoS Access	Y	-	Y	Y	Allow portlet users to browse QoS series.
Reassign	Y	-	-	Y	Override assignment at Assign/Acknowledge.
Report Designer	Y	-	-	Y	Create, modify, and delete reports.
Report Scheduler	Y	-	Y	Y	Access to ReportScheduler portlet.
Service Desk	Y	-	Y	Y	Access to Service Desk and My Tickets portlets.
SLM Admin	Y	-	-	Y	Run Service Level Manager with full access.
SLM View	Y	-	Y	Y	Run Service Level Manager in read-only mode.
SLO Access	Y	-	Y	Y	Allow portlet users to browse SLO data.
Unassign	Y	-	-	Y	Unassign alarms.
Unified Reports	Y	-	-	Y	Access to Unified Reports.

User Administration	Y	-	-	Y	Create, modify, and delete users.
User Customization	Y	Y	Y	Y	Customize own portal content.
User Monitoring	Y	-	-	Y	Display and disconnect user sessions.
USM Automatic Robot Installation	Y	-	Y	Y	Automatically deploy and install robots to targeted system.
USM Basic	Y	Y	Y	Y	Access to USM portlet.
USM Edit Monitoring Station Groups	Y	-	Y	Y	Create, edit, and delete monitoring station groups.
USM Edit Monitoring Templates	Y	-	Y	Y	Create, edit, and delete monitoring templates.
USM Geo View Modification	Y	-	Y	Y	Create, edit, and delete geo views.
USM Group Modification	Y	-	Y	Y	Create, edit, and delete groups.
USM Modify Individual Monitors for Computer Systems	Y	-	Y	Y	Create, modify, and delete individual SOC monitors.
USM Self Service Monitoring	Y	-	Y	Y	Enable or disable out-of-box monitoring template.
Web Publish	-	-	-	Y	CA UIM Server HTML management.
Web service	Y	-	-	Y	Access to CA UIM Web Service API.

Permissions Reference for UMP Portlets

To access UMP portlets, users must have the appropriate permissions set in the Access Control List (ACL). ACL permissions are set in the Account Admin portlet. A "permission denied" message is displayed when users try to access a porlet for which they do not have the required permission.

Note: The SLM portlet does not allow access to account contact users, regardless of permissions set.

Account Admin

Required Permission for Access:

- Account Administration

Other Available Permissions:

- Manage ACL - create, modify, and delete ACLs.

Change Password

Required Permission for Access:

- Change Password

Note: In addition to having the Change Password permission set in the ACL, the user must be an account contact user in order to access this portlet.

Cloud Monitor

Required Permission for Access:

- Cloud UE Monitor

Dashboard

Required Permission for Access:

- Dashboard Designer - allows bus users to create, edit, and publish dashboards
- Custom Dashboards - allows account contact users to view dashboards

Discovery Status

Required Permission for Access:

- Discovery Pie

List Designer

Required Permission for Access:

- List Designer

List Viewer

Required Permission for Access:

- List Viewer

My Tickets

Required Permission for Access:

- Service Desk

NetFlow

Required Permission for Access:

- Netflow

Performance Reports Designer

Required Permission for Access:

- QoS access

Reports

Required Permission for Access:

- Custom Reports

Report Scheduler

Required Permission for Access:

- Report Scheduler

Service Desk

Required Permission for Access:

- Service Desk

SLA Reports

Required Permission for Access:

- SLM View

SLM

Required Permission for Access:

- SLM Admin

Unified Reporter

Required Permission for Access:

- Unified Reports

Unified Service Manager

Required Permission for Access:

- USM Basic or Basic Management

Note: The Basic Management permission allows users to take actions in other CA UIM applications, such as starting and stopping probes in Infrastructure Manager. Use the USM Basic permission to grant USM access while restricting access to other areas of CA Unified Infrastructure Management.

Other Available Permissions:

- USM Edit Monitoring Templates
- USM Group Modification
- USM Automatic Robot Installation
- USM Modify Individual Monitors for Computer Systems
- Probe Configuration ACL permission to launch a probe configuration GUI for an interface
- Edit Maintenance Mode Devices
- Edit Maintenance Mode Schedules
- Alarm Management - enter text for alarms in five custom fields (by default named **Custom 1** through **Custom 5**).
- Invisible Alarms - see invisible alarms and set alarms to be invisible.
- Alarm action permissions:
    - Accept
    - Acknowledge (clear)
    - Assign
    - Unassign

System Access

This section describes how users and systems can interact with CA UIM.

CA UIM Interfaces

You can access information in CA UIM through the following interfaces:

- **Admin Console**
  A web-based management console that allows you to manage your CA UIM infrastructure on virtually any desktop or server operating system. Admin Console can also be run within a portlet in Unified Management Portal (UMP). Admin Console portlet is installed during the UMP installation.
  Users with administrator or superuser permissions can access Admin Console.
- **RESTful Web Services**
  A Representational State Transfer (RESTful) web service interface for CA UIM. This interface offers customers the functionality to access their CA UIM installation using REST-based web service calls.
- **Infrastructure Manager**
  A Windows-based interface that lets you configure and manage your CA UIM deployment. It provides:
    - A hierarchical view of systems being monitored
    - An alarm window to view all alarms and messages

    - Interfaces that allow you to configure your hubs, robots, and probes

  Infrastructure Manager connects to an active hub and allows you to control, configure, and manage the robots and probes in your deployment.

- **Unified Management Portal** (UMP) is a web-based portal that lets you discover devices and view your data, alarms and messages in a variety of ways.

Hub Port Requirements

The ports that are required for a successful infrastructure installation depend on how you configure the hubs in your environment. If we assume the default first port of 48000 is used, port assignments are as follows:

- Single-hub infrastructure or multiple-hub infrastructure that does NOT use tunnels:
  - **48000** for the robot controller probe
  - **48001** for the robot spooler probe
  - **48002** to allow robot-to-hub and manager-to-hub communications
  - A port for each probe you install; these ports start at **48004** and are assigned to each probe as the probe is activated
  - **8080** (service_host) default port to access Admin Console and CA UIM web page through HTTP
  - **8443** (service_host) default port to access Admin Console and CA UIM web page through HTTPS
- Multiple-hub infrastructure that uses tunnels that are NOT SLL tunnels:
  - All ports that are used in a single-hub installation
  - **48003** for the tunnel server (can also be set to 443)
- Multiple-hub infrastructure that uses SSL tunnels:
  - **48000** (controller) and **48002** (hub)
  - **48003** to allow the tunnel client to access the tunnel server
  - **8443** and **8080** (service_host) to allow the tunnel client to access Admin Console and CA UIM web page

Probe Port Requirements

Some probes have additional port requirements. For example:

- The udm_manager probe uses port 4334 by default to communicate with udm clients (datomic peers).
- The snmpcollector probe uses port 161 by default to communicate with the SNMP port on a device.

For information about probe specific port requirements, refer to the probe documentation. The information for CA Unified Infrastructure Management Probes is available on the CA Unified Infrastructure Management Probe Space.

HTTPS Configuration

During the initial installation of CA UIM Server, HTTP access to the CA UIM Server webpage and Admin Console is configured on port 8080. To implement a secure connection using HTTPS, see Configure

HTTPS in Admin Console. The default port for HTTPS configuration in Admin Console is 8443. After you configure HTTPS in Admin Console, port 8080 is not required.

During the initial installation of UMP, HTTP access to the UMP portal is configured on port 80. To implement a secure connection using HTTPS, see Configure HTTPS in UMP. The default port for HTTPS configuration in the UMP portal is 443. After you configure HTTPS in the UMP portal, port 80 is not required.

CA UIM Installer Creates the Database Schema and User

This article describes the steps that are required to configure the UIM database before CA UIM installation.

Tip: If you have questions regarding which database vendor software is supported with CA UIM, refer to the Compatibility Support Matrix. For general database installation procedures, refer to the product documentation provided by your database vendor.

Determine Your Database Creation Method

Determine the method that is used to create the UIM database before you run the UIM Server installer. Once you have chosen a creation method, follow the instructions for your database software.

The UIM Server Installer Creates the Database Schema

The UIM Server installer can create the UIM database as part of the installation process. If you use this method, the UIM installer requires access to a database account with administrator privileges. Examples include:

- root in MySQL
- sa in Microsoft SQL Server
- SYS in Oracle

When you run the installer, enter the credentials for designated account.

If you use this installation method, skip the **Manual Creation of the Database Schema (or Tablespace) and User** section for your database software.

Manual Creation of the Database Schema and User

If you do not want to give the UIM Server installer access to an administrator account, you can create the UIM database and associated user manually. We recommend manual database creation in environments that have a dedicated database administrator. Before you install UIM Server, verify that the created user is the schema owner in Oracle or MySQL instances, or the Database Owner (DBO) in Microsoft SQL Server instances. Also, verify that the user is granted all permissions for the schema. If you create the database and user in advance, click **Use existing database** when prompted by the CA UIM installer.

Important! We recommend that you begin with a fresh database installation on a clean system. Using a pre-existing database can cause subtle configuration conflicts that are hard to diagnose.

Microsoft SQL Server

CA UIM supports only the full licensed product version with database authentication or Windows authentication for production environments. To obtain a copy of Microsoft SQL Server go to www.microsoft.com/sqlserver and follow the installation instructions available with the download.

Note: Both the Enterprise and Standard Editions of Microsoft SQL Server are supported with CA UIM. However, we generally recommend that you use the Enterprise Edition.

When installing Microsoft SQL Server, the simplest solution is to:

- Accept the default instance name when you install Microsoft SQL Server
- Use the default port (1433) when you install CA UIM
- Run the installer as the domain logon user to be associated with the CA UIM Server installation.

Other solutions have different requirements. If you:

- **Use a non-default instance name for the Microsoft SQL Server:** Use the default port (1433) when installing CA UIM.
- **Use a port other than 1433 for CA UIM:** Use the default Microsoft SQL Server instance name.

During UIM server installation you can select one of the following authentication options:

- **SQL Server with SQL Server login**: Provide the SQL server user name and password during installation. No modifications are needed.
- **SQL Server with Windows authentication**: You might need to make database modifications in advance, as described in the next section.

Requirements for Windows NT Authentication

If you are also using Windows Authentication:

- Enable the SA account and set the password. For instructions, go to https://msdn.microsoft.com/en-us/library/ms188670.aspx.
- Add a domain administrator with permission to **Log on as a Service** on both the CA UIM system and the database system. For instructions, go to http://technet.microsoft.com/en-us/library/dd277404.aspx.
- Configure SQL server to use Windows authentication. For instructions, go to http://msdn.microsoft.com/en-us/library/aa337562.aspx.

Note: The user installing CA UIM must have the same administrative rights that were used to install the SQL server. Specifically, the data_engine probe must have identical administrative rights on both the CA UIM system and the database system. These credentials are supplied during installation.

Manual Creation of the Database Schema and User

Follow these steps:

1. Log in to SQL Server Management Studio as the system administrator (sa).
2. Execute the following commands individually:
3. `CREATE DATABASE <UIM_db_name>;`
4. `USE <UIM_db_name>;`
5. `CREATE LOGIN <UIM_db_user> with PASSWORD ='<UIM_db_password>', DEFAULT_DATABASE = <UIM_db_name>;`
6. `CREATE USER <UIM_db_user> FOR LOGIN <UIM_db_user>;`
7. `EXEC sp_addrolemember ‘db_owner’, <UIM_db_user>;`
   `EXEC sp_addmessage @msgnum = 55000, @severity = 16, @msgtext = N'%', @replace = 'replace', @lang = 'us_english';`

MySQL Server

You can obtain a copy of the open source MySQL database software from http://dev.mysql.com/downloads/. You can use either the Community Server version or a licensed version.

MySQL variables must be set as follows:

- **lower_case_table_names=1**
- **local_infile=ON**

While not typically required, we recommend that you also set the following variables:

- **log_bin=ON**

  Important! If you are using replication or certain data recovery operations, binary logging is required. See your MySQL documentation for details.

- **log_bin_trust_function_creators=ON** (if log_bin is set to **ON**)
- **binlog_format=mixed** (if log_bin is set to **ON**)

Use the following procedure to view the setting for each variable.

Follow these steps:

1. Log in to the MySQL server as the administrator.
2. For each variable, execute:
3. `show variables like 'variable_name';`
4. If a variable is incorrect or missing, edit the MySQL server configuration file as instructed in your MySQL documentation.
5. Restart the database if you made any changes,

MySQL in Large Environments

If you are preparing for a large-scale or major deployment, you can change more database parameters to allow for greater demands of such an environment. We recommend that you begin with the values shown in the following example, and then fine-tune settings depending on your circumstances.

As the MySQL administrator, add these lines to the MySQL server configuration file:

```
[mysqld]
max_heap_table_size=134217728
query_cache_limit=4194304
query_cache_size=268435456
sort_buffer_size=25165824
join_buffer_size=67108864
max_tmp_tables=64
```

Manual Creation of the Database Schema and User

Follow these steps:

1. Log in as the MySQL administrator.
2. Create the database. Execute:

   ```
   CREATE DATABASE IF NOT EXISTS <uim_db_name> DEFAULT CHARACTER SET = utf8
   DEFAULT COLLATE = utf8_unicode_ci;
   ```

   Where *<uim_db_name>* is the desired database name

3. Create the user and assign required privileges. Execute:
4. `CREATE USER '<uim_db_owner>'@'%' IDENTIFIED BY '<uim_db_owner_password>';`
5. `GRANT ALL PRIVILEGES ON <uim_db_name>.* TO 'uim_db_owner'@'%';`
   `FLUSH PRIVILEGES;`

   Where *uim_db_owner* is the desired user name for the owner, *uim_db_owner_password* is the desired password, and *uim_db_name* is the name of the database you created.

   Note: The single-quotation marks (') are required.

Oracle

The Oracle Instant Client must be installed on the CA UIM system so it can access the Oracle database.

Follow these steps:

1. Go to www.oracle.com and click **Downloads, Instant Client**.
2. Click the link for the operating system and hardware of your system.
3. Download the zip file for the **Instant Client Package - Basic**.
4. Install the Instant Client according to the directions on the web site. The UIM installer asks for the location of the Instant Client.
5. Restart the system.

The Oracle administrator must also set the following required configuration parameters before installing CA UIM.

Follow these steps:

1. As the Oracle database administrator, execute:
2. `ALTER SYSTEM SET PROCESSES = 300 SCOPE=SPFILE;`
3. `ALTER SYSTEM SET SESSIONS = 335 SCOPE=SPFILE; -- 1.1 * PROCESSES +5`
4. `ALTER SYSTEM SET OPEN_CURSORS = 500 SCOPE=BOTH;`

5. Restart the database.

Configure Settings for Oracle Shared Server

If your Oracle database is configured for shared server use, you can increase the total number of allowed shared server sessions using the **SHARED_SERVER_SESSIONS** parameter. Generally, we recommend increasing the **SHARED_SERVER_SESSIONS** to 300 as a starting point.

Important! The error message **ORA-00018: maximum number of sessions exceeded** during UIM installation indicates that the number of allowed shared server sessions should be increased.

(UMP Only) Turn off the Oracle Recycle Bin

If you will install the Unified Management Portal (UMP), then the recycle bin must be turned off before you install UIM Server.

Follow these steps:

1. Use a tool such as SQL Developer to connect to the Oracle database.
2. Enter the following commands:
3. `ALTER SYSTEM SET recyclebin = OFF DEFERRED;`
4. `ALTER SESSION SET recyclebin = off;`
5. Verify that the recycle bin is off using the following command:
6. `show parameter recyclebin;`

Note: We do not recommend turning the Oracle Recycle Bin back on after installing UMP.

Verify Linking for Shared Oracle Libraries on Unix Systems

Shared Oracle libraries on Unix-based systems must be linked.

Follow these steps:

1. Go to the instant client.
2. Execute:

```
ldd libociei.so
```

3. Verify that there are links for all the libraries and that there are no **not found** messages. The output should look similar to the following:

```
4. linux-vdso.so.1 +> (0x00007fff5b0e2000)
5. libclntsh.so.11.1 => /root/instantclient_11_1/libclntsh.so.11.1
   (0x00007f36030b3000)
6. libdl.so.2 => /lib64/libdl.so.2 (0x00007f3602eae000)
7. libm.so.6 => /lib64/libm.so.6 (0x00007f3602c57000)
8. libpthread.so.0 +> /lib64/libpthread.so.0 (0x00007f3602a3a000)
9. libnsl.so.1 => /lib64/libnsl.so.1 (0x00007f3602821000)
10. libc.so.6 => /lib64/libc.so.6 (0x00007f36024c1000)
11. libnnz11.so => /root/instantclient_11_1/libnnz11.so (0x00007f3602064000)
12. libaio.so.1 => /lib64.libaio.so.1 (0x00007f3601e61000)
    /lib64/ld-linux-x36-64.so.2 (0x00007f360a0a0000)
```

Manual Creation of the Tablespace and User

The procedure for creating a tablespace manually depends on the version of Oracle that you are using.

Oracle 12c

Create a pluggable database using the files of a seed database. See the Oracle documentation for details about the options available when you create a database from a seed.

Follow these steps:

1. Log in to the desired Oracle database as the administrator (sys as sysdba).
2. Create a pluggable database. Execute the following statement, where <*pdb_name*> is the name of a pluggable database and <*ts_name*> is a tablespace name of your choice (for example, *uim_ts)*:

```
3. create pluggable database <pdb_name> admin user <db_owner> identified by
   <owner_password>
4.     default tablespace <ts_name>
5.     datafile '<data_file_full_name.dbf>' size 500m autoextend on
6.     file_name_convert = ('<location_of_db_to_be_cloned>',
   '<location_of_new_pluggable_db>');
   alter pluggable database <pdb_name> open;
```

7. Connect to the pluggable database using 'sys as sysdba'. The service name for the pluggable database is the <*pdb_name*> created in the previous step.
8. Create a non-administrator user in the UIM pluggable database. Execute the following statement, where <*non-admin_owner*> is the name of the user to be created:

```
create user <non_admin_user> identified by <user_password>;
```

9. Grant the necessary privileges to the local user <non_admin_user>.

```
10. grant unlimited tablespace to <non_admin_user>;
11. grant administer database trigger to <non_admin_user>;
12. grant create table to <non_admin_user>;
13. grant create any table to <non_admin_user>;
14. grant create view to <non_admin_user>;
15. grant alter any table to <non_admin_user>;
16. grant select any table to <non_admin_user>;
17. grant create sequence to <non_admin_user>;
18. grant create procedure to <non_admin_user>;
19. grant create session to <non_admin_user>;
20. grant create trigger to <non_admin_user>;
21. grant create type to <non_admin_user>;
22. grant drop any table to <non_admin_user>;
23. grant lock any table to <non_admin_user>;
24. grant select on sys.v_$session to <non_admin_user>;
25. grant execute on sys.dbms_lob to <non_admin_user>;
26. grant execute on dbms_redefinition to <non_admin_user>;
```

27. Start the UIM Server installer. When prompted, enter the following information:

-
  - **Service Name**: Name of the pluggable database instance <*pdb_name*> you created

- **Port**: Port of the Oracle database
- **Username**: Username for local user *<non_admin_user>*

Your database server is ready.

Oracle 11g or Earlier

Follow these steps:

1. Log in as the Oracle administrator.
2. Create the tablespace. Execute the following statement, where *<ts_name>* is a tablespace name of your choice (typically *CA_UIM)*:

   ```
   create tablespace <ts_name> datafile '<ts_name>.dbf' size 1000m autoextend on
   maxsize unlimited;
   ```

3. Create the owner and assign required privileges. Execute the following statement, where *<db_owner>* is the name of the user to be created and *<ts_name>* is the tablespace:

```
4. grant unlimited tablespace to <db_owner>;
5. grant administer database trigger to <db_owner>;
6. grant create table to <db_owner>;
7. grant create view to <db_owner>;
8. grant alter any table to <db_owner>;
9. grant select any table to <db_owner>;
10. grant create sequence to <db_owner>;
11. grant create procedure to <db_owner>;
12. grant create session to <db_owner>;
13. grant create trigger to <db_owner>;
14. grant create type to <db_owner>;
15. grant select on sys.v_$session to <db_owner>;
16. grant execute on sys.dbms_lob to <db_owner>;
17. grant execute on dbms_redefinition to <db_owner>;
18. grant create any table to <db_owner>;
19. grant drop any table to <db_owner>;
    grant lock any table to <db_owner>;
```

   Note that:

   - The owner and tablespace commonly have the same name.
   - The *grant unlimited tablespace* command sets the quota for all tablespaces to unlimited. Although not tested by CA, you can set the quota for only the UIM database by executing the following statement in place of *grant unlimited tablespace to <db_owner>*:

     ```
     alter user <db_owner> quota unlimited on <ts_name>;
     ```

Software Installation and Upgrades

Download CA UIM software from support.nimsoft.com. Log on to the website and go to **Downloads**. You must have Administrator permissions on a system to install CA UIM and UMP. For more information, see Upgrading & Release Notes.

Installation Parameters

This article describes the parameters that are used during CA UIM installation. The parameters that are required during your installation vary depending on:

- The installation method that you are using.
- The database software that you are using for the UIM database.

GUI and Console Parameters

The GUI and console installation processes prompt you for the parameters that are required for your operating system and database.

MySQL Parameters (GUI/Console)

Parameter	Value
Database Server Hostname or IP	Database server hostname or IP address
Database Server Name	Desired name for a new database, or the name of the UIM database that is created before UIM Server installation
Database Port	Database server port (typically 3306)
Database Name	Enter **CA_UIM** or the name of your choice
Database Username **Database Password**	Database administrative account (root) and password

SQL Server Parameters (GUI/Console)

Parameter	Value
Database Server Hostname or IP	Database Server hostname or IP address
Database Server Port	• Database server port if the port is assigned (default is 1433) • 0 or leave blank if using dynamic ports
Database Name	• CA_UIM (default) or name of your choice for a new database • Actual name of the UIM database that is created before UIM Server installation
Database Authentication Mode	• SQL Server Authentication to use the database to authenticate credentials • Windows Authentication to use Active Directory to authenticate credentials

Database Username	• Username for a SQL Server user account on the database server if you chose SQLServer Authentication (default is **sa**) • Domain/username for a Windows account if you chose Windows Authentication **Note:** If you chose **Create New Database** mode, this account must have administrative privileges.
Database Password	• Password for existing database administrator account • Desired password if the account is created during CA UIM installation.

Oracle Parameters (GUI/Console)

Parameter	Value
Oracle Instant Client Directory	• Location of Oracle Instant Client (required)
Database Server Name	• Hostname • IPv4 address
Database Server Port	• Database server port (typically 1521)
Database Service Name	• Oracle service name to use for the database connection (default is ORCL) • (*oracle 12 ONLY)* Pluggable database name
SYS Password	• Password for the SYS account on the database server (required only if database is created during installation)
Database Username	• Desired name for the UIM database user account that the installer creates (new) • Database user who is created when database was created (existing)
Database Password	• Password for the UIM database administrator account
Database Tablespace Name	• Tablespace name to associate with the database username schema. Valid characters are: a-z, A-Z, 0-9 and underscore (_)

Hub Parameters (GUI/Console)

Parameter	Value
Domain Name	• Desired domain name (default is *hostname*_domain)
Primary Hub Name	• Desired hub name (default is *hostname*_hub)

Primary Robot Name	• Desired robot name (default is *hostname*)
Primary Robot First Probe Port	• No value or the default (**48000**) • Port assignments start at 48000. Increase by one until a free port is found, then continue to increase for subsequent assignments • Any available port if you want to specify an initial port for UIM probes. Subsequent port assignments increase from the specified port
Primary Hub IPv4 Address	• IP address that you want to use for UIM traffic (the installer displays all network interfaces attached to the computer)
Primary Hub License	• License key exactly as it appears on your UIM License Document • **Autogenerated** to create a temporary license that is valid for 30 days
UIM Administrator Username	• **Administrator** by default
UIM Administrator Password	• Desired UIM administrator password (at least six characters)

Silent Install Parameters

Silent install parameters are defined in the **installer.DB_OS.properties** file. Parameters for all platforms are listed in this section. Only the parameters included in each section are required for the specified OS.

Database Parameters (Silent)

The database parameters are described in the **uimserver_silentinstall_master.properties** file. Parameters for all databases are listed in this file. Only the parameters included in each section are required for the specified database.

UIM Server Parameters (Silent)

The UIM Server parameters are described in the **uimserver_silentinstall_master.properties** file. Parameters for the UIM Server are listed in this file.

Optional Post-Installation Tasks

Once you have completed setting up your CA UIM environment, you can complete several optional post-installation tasks.

- Encrypt UIM Network Traffic with SSL
- Enable Login with LDAP
- Configure HTTPS in Admin Console
- Configure HTTPS in UMP
- Configure UMP to Use SAML Single Sign-On
- Set Up Access to UMP Using a DMZ