GENESYS
AN ALCATEL·LUCENT COMPANY

Informiam
Product Line

Frontline Advisor and Agent Advisor Installation Guide (Windows)

Release 3.3
April 1, 2010

Table of Contents

Change History

Date	Changed by	Comments
Dec. 19, 2007	Diane	incorporated Yuxiao's changes for 2.8.4
June 02, 2008	Jamie	Major content update for 2.9.2.
June 18, 2008	Diane	copy edit
June 19, 2008	Kirt	Adding screen shots from begin to end
July 10, 2008	Kirt	Making another pass using build 11
August 8, 2008	Kirt	Another pass after input from other people
August 18, 2008	Diane	copy edit
October 27, 2008	Diane	As per Alla, changed informiam_hadb_hierarchy informiam_fadb_stg
November 11, 2008	Diane	Changes as per Yevgeny (from Twiki)
November 28, 2008	Diane	Added Modules to Install and Hierarchy Staging Database Configuration screens
December 4, 2008	Diane	Moved *Configuring Memory Allocation* to the Platform installation guide. Updated *Starting the Frontline Advisor Service.* Removed *Conflicting AJP Ports* since we're using the Platform Geronimo Server instead.
Jan 16, 2009	Diane	update version numbers to 3.1; Agent Advisor; copyright
March 31, 2009	Diane, Charles	• fa-new-installer-<version>.jar should be fa-server-installer-<version>.jar • Remove *Uninstalling FA*, fa-stg-mssql, and fa-custom-metrics content • As long as the login name specified matches the FA_HIER_Person.LoginName field in the hierarchy database, the CA database record will be updated rather than inserted. • The default hierarchy db is informiam_fadb_hierarchy • FA_HIER_Person: Fname nvarchar(128), Lname nvarchar(128), LoginName nvarchar(50) • FA_HIER_Team: EnterpriseName nvarchar(128) • FA_HIER_Agent and FA_HIER_Agent_Team_Member: AgentSkillID varchar(500) • The FA user should be given only the following roles: db_datareader, db_datawriter, db_ddladmin roles (not db_owner). Add *Truncating the Violations Table* and *Changing the Values at the Enterprise Node*
March 11, 2010	Charles	• Updated for 3.3 • Migration scripts • Custom Metrics Module
March 23, 2010	Victoria, Charles	• Typographical error corrections

1.   Overview

This document specifies how to install Frontline Advisor and the Agent Advisor v3.3 in a Windows 2003 Server environment. Note that version numbers in the final release may be different than those in the screen captures in this document.

Prerequisites

Advisors Platform v.3.3.0 and Apache HTTP Server 2.2 must be installed and configured before doing the work described in this document. See the Advisors_*Platform_InstallationGuide_3.3.000GA.pdf*The Release Notes specify the latest Advisor supported versions. The third party software prerequisites include:

- Java 6 SDK (JDK 1.6)
- Microsoft SQL Server 2005
- Acrobat Reader

Changes from 3.1.0

- Custom Metrics Module can be installed as a companion application
- Migration scripts are introduced to ease database updgrades

Changes from 3.0.0

The installer will not upgrade an older version of Frontline Advisor to version 3.1.0. Any existing version of Frontline Advisor must be uninstalled before installing Frontline Advisor version 3.1.0.

Changes from 2.9.0

- Frontline Advisor uses Platform 3.0 security.
- Geronimo 1.1.1 is installed as part of Platform 3.0.
- Frontline Advisor installer is replaced with ANT Installer.
- The Monitoring Hierarchy is now multi-level and is imported from a new separate database.
- Apache HTTP Server is required to route requests from the Informiam Browser to the Frontline Advisor server (Geronimo)

2.   Installation Summary

Installation Contents

The following files are shipped with the Frontline Advisor distribution.

fa-distribution-3.3.000.<build#>.zip\ip

- fa-hierarchy-mssql-3.3.000.<build#>.sql
- database script: fa-new-database-3.3.000.<build#>.sql
- server installer: gfa-server-installer-3.3.000.<build#>.jar
- migrations folder
    - fa_mssql_ddl_3.1.sql
    - fa_mssql_initial_upload_3.1.sql
    - fa-database-migration-3.1-to-3.3.sql
    - hierarchy_mssql_ddl_3.1.sql
    - hierarchy-migration-3.1-to-3.3.sql

- Supplemental folder
    - RemoveFAUsersFromFA.sql
    - SetObjectLevelPermissions.sql
    - DropAllFADBObjects.sql
    - PopulateHierarchy.sql
    - CleanCmmConfigsAtFadb.sql

Installation Steps

The installation steps are:

- Creating the Frontline Advisor Database, see Section 3
- Creating the Monitoring Hierarchy Database, see Section 4
- Installing the Frontline Advisor Server, see Section 5
- Populating the Monitoring Hierarchy Database, see Section 6
- Starting the Frontline Advisor Service, see Section 7
- Configuring Apache Routes, see Section 8
- Verifying Server Connections, see Section 9

Optional Configuration

- External Link In Link Out URL parameters, see Integrating External Links.
- Installing and configuring custom metrics, see "Custom Metrics Module"

Notes

If you **must** define users in the Advisors Platform database: the login name must match the FA_HIER_Person.LoginName field in the hierarchy database, the Platform database record will be updated rather than inserted. For more information, see *Monitoring Hierarchy Importer* in page 25.

The very first time Frontline Advisor is started, the entire Monitoring Hierarchy is imported from the source that was defined during installation. This may take some time, do not stop or restart the server during this time.

3. Creating the Frontline Advisor Database

Note: If due to security restrictions administrator access cannot be granted, have the customer's DBA implement the steps described in the section, Creating a Login to be Used by Frontline Advisor.

The following steps should be followed when installing a Frontline Advisor database from scratch. For instructions on updating a Frontline Advisor database from an earlier version, see "Migrating Frontline Advisor Database" below.

To create the FA database:

1. Connect to the SQL Server 2005 instance using Microsoft SQL Server Management Studio with the LoginId assigned to the SQL Server sysadmin server role. It can be "sa" or any other login assigned to the sysadmin server role and created for you by the customer's DBA for temporary use during the deployment.

2. In the object explorer right click on Databases and choose New Database. Open the General page (Figure 1).

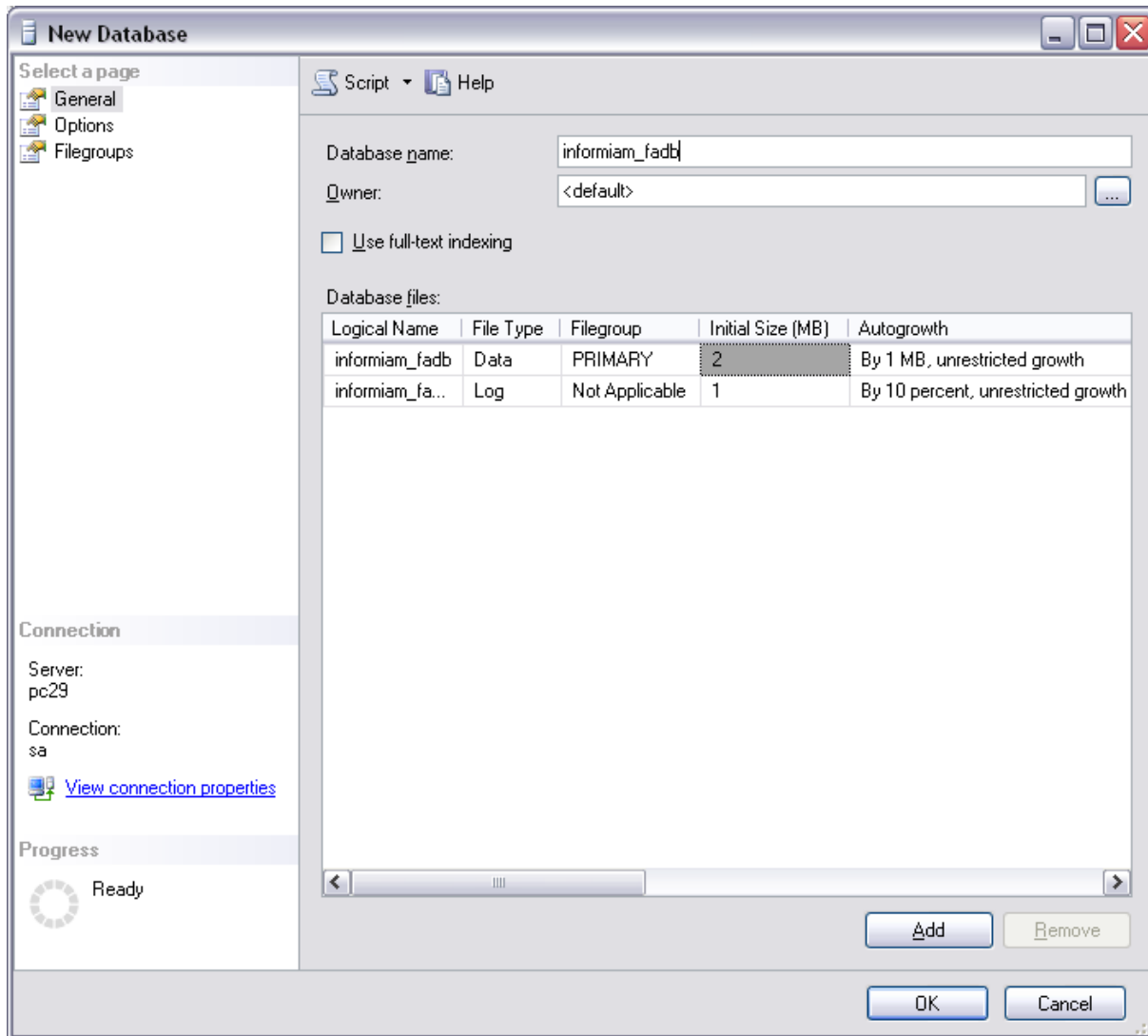*Figure 1: Database Properties. General*

a) Specify the database name.

b) Leave the owner as <default>.

c) Specify 50 MB as the initial data file size with growth by 10%, unrestricted file growth.

d) Specify 150 MB as the initial log file size with file growth by 5 MB, unrestricted file growth.

e) Change paths to the data and log files if necessary.

3. Open the Options page (Figure 2).
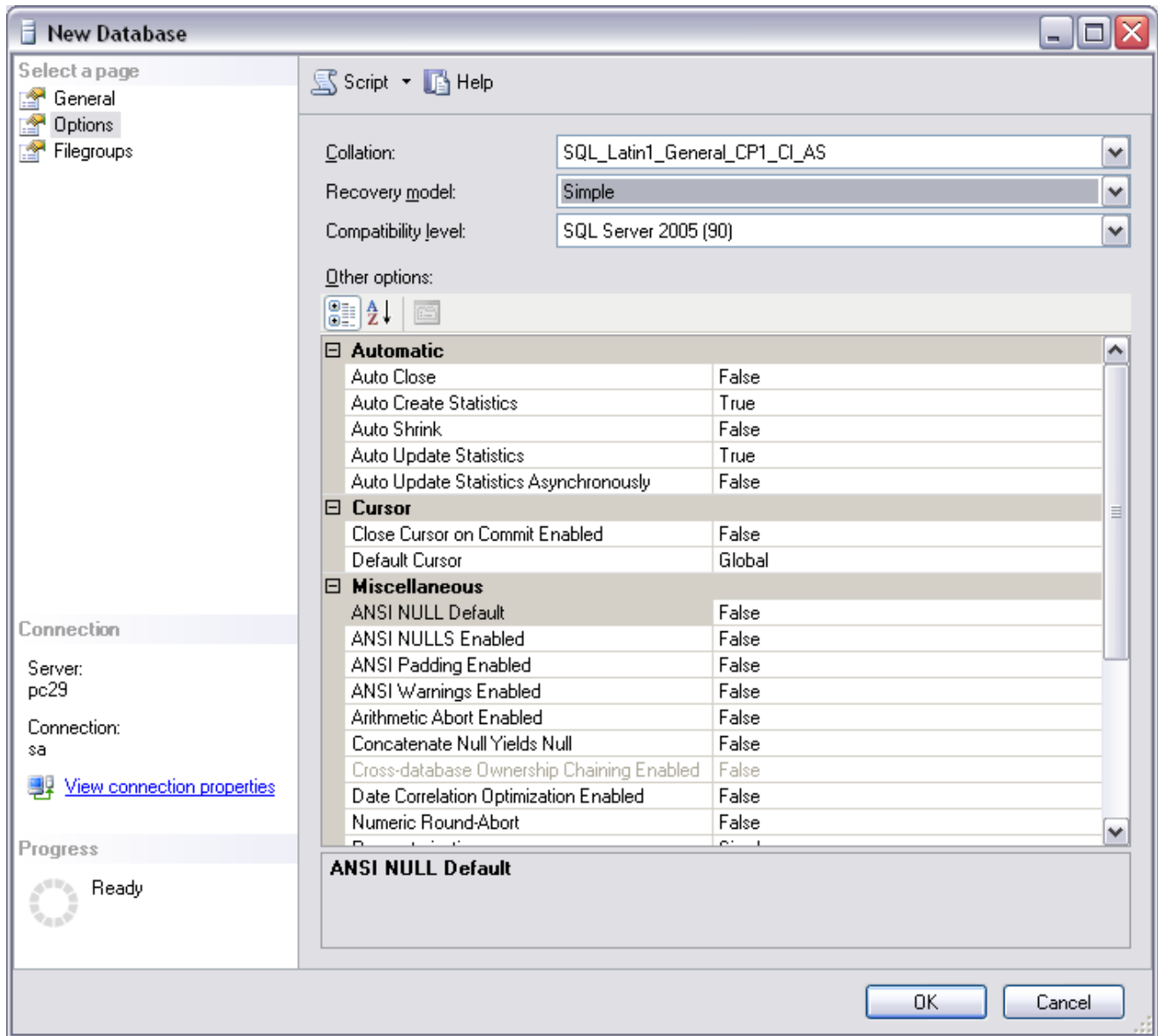
Figure 2: Database Properties, Options

   a) Select SQL_Latin1_General_CP1_CI_AS for the collation.

   b) Select Simple for the recovery model.

   c) Set Auto Create Statistics and Auto Update Statistics as True.

4. Click OK.

5. Click OK (2). The database is created and properties are configured.

Creating a Login to be Used by Frontline Advisor

1. In the Microsoft SQL Server Management Studio object explorer choose Server |

Security page.
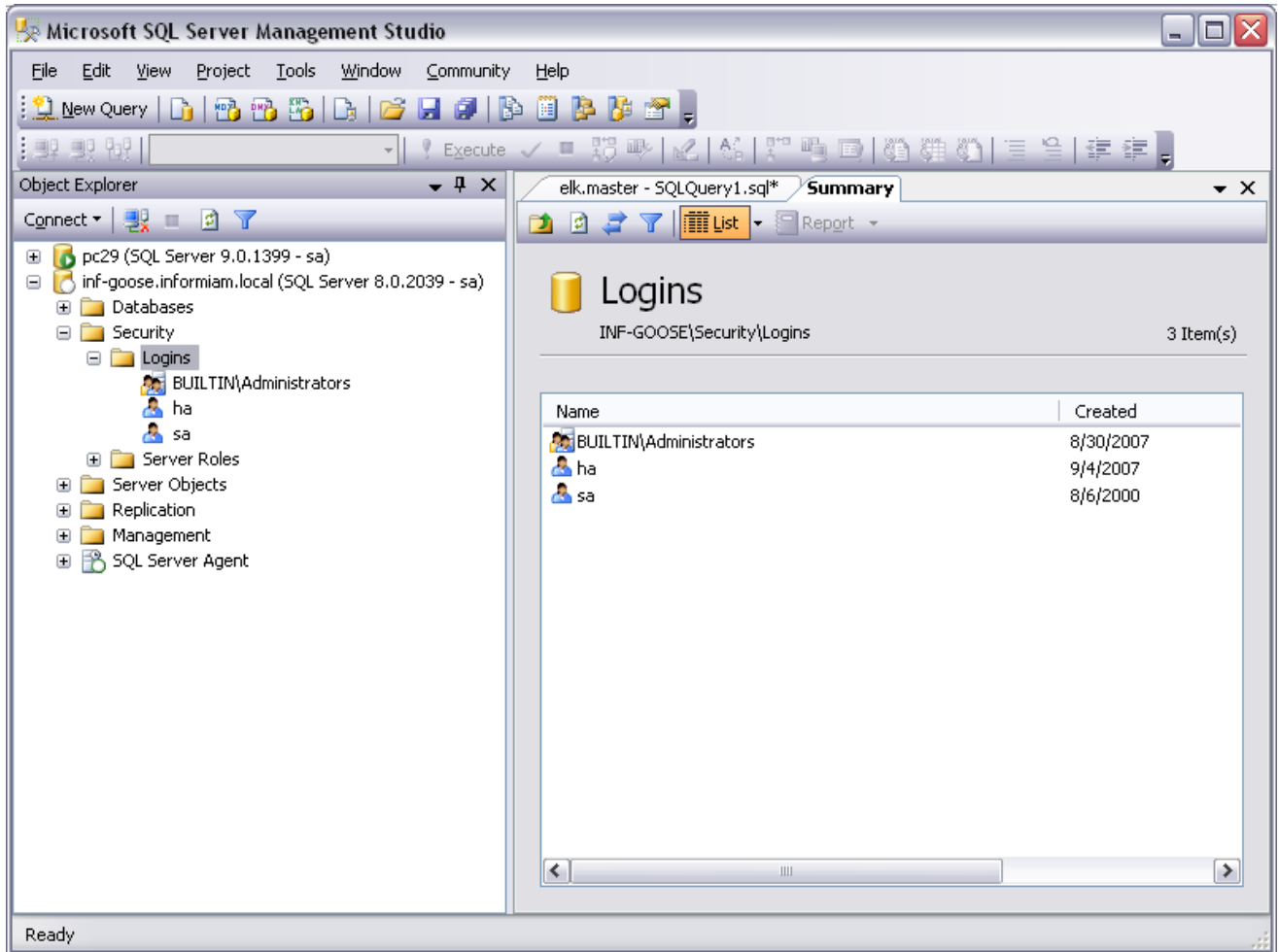
Figure 3: Server Level Security

2. Right click Logins and choose New login.
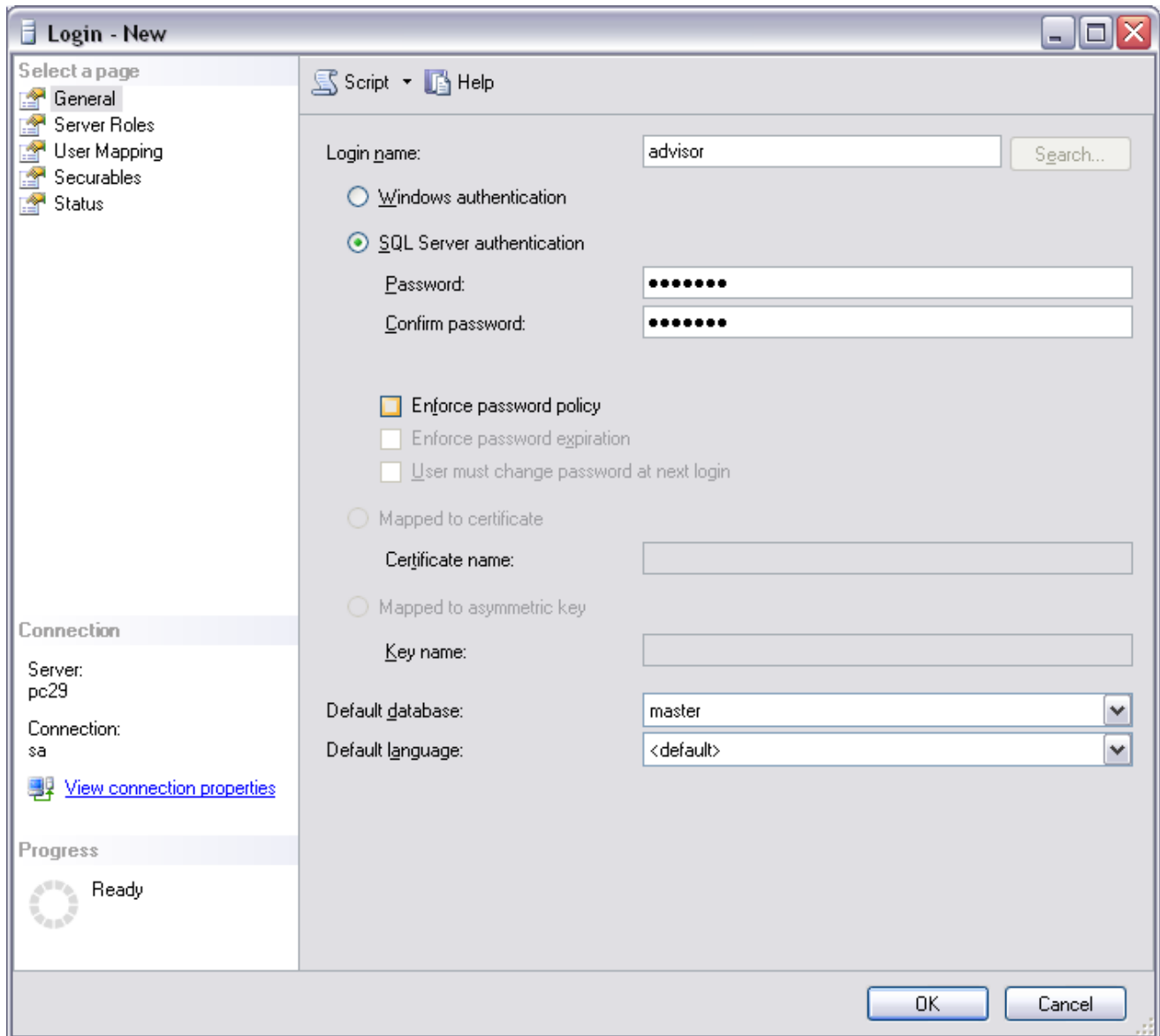
Figure 3: SQL Server Login Properties - New Login

3. Open the General page (Figure 3).

   a) Specify the login name (in this example advisor).

   b) Select the SQL Server Authentication radio button.

   c) Specify a password that complies with the organization's security policy.

   d) If strong passwords are part of the security policy, select the Enforce password policy check box.

   e) Set master as a default database

   The login to be used by Frontline Advisor is created and configured.

   The same login must be mapped to the Hierarchy database user.

4. Using Windows Explorer, navigate to the Frontline Advisor fa-new-database_xxx.sql file for your release.
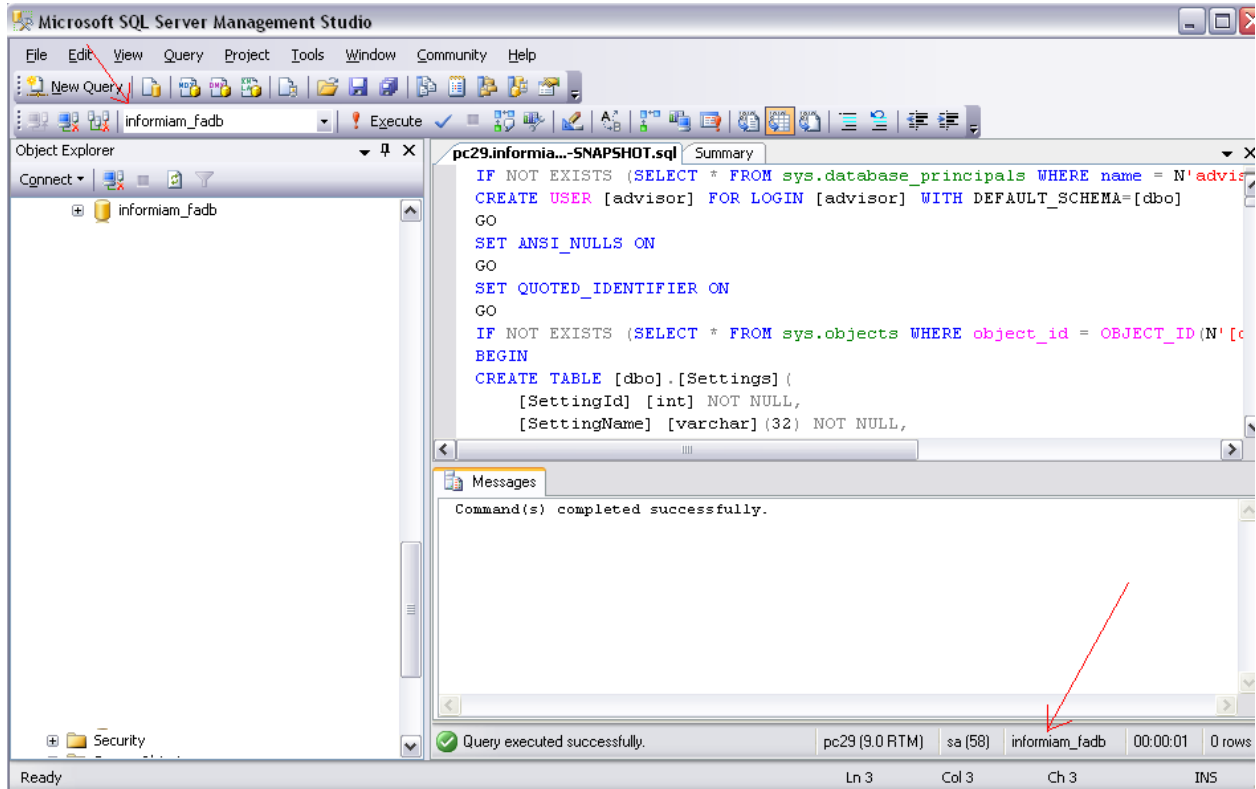
Figure 4: SQL Server Management Studio

5. Open the sql file in the New Query window. Select the created database from the drop-down list and make sure that its name displays in the bottom of the query window (Figure 4).

6. Run the script and make sure that the result is successful.

7. Navigate to Security / Users.

8. Right-click on advisor.

9. Choose Properties.
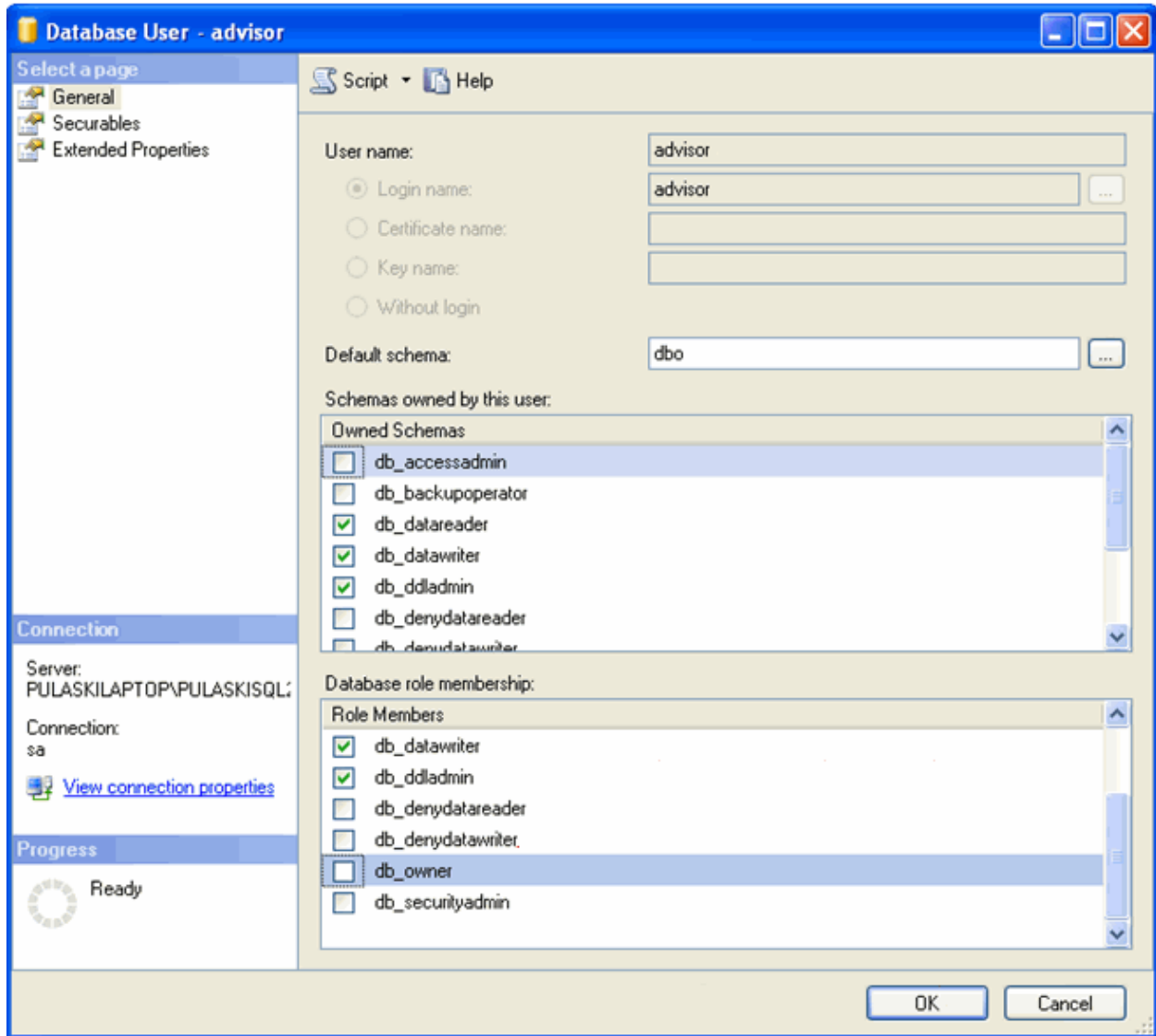
Figure 5: Database User

10. Make sure the advisor user is defined as follows: the login is advisor; the default schema is dbo; the db_datareader, db_datawriter and db_ddladmin options are selected (Figure 5). Set explicit permissions to execute all stored procedures and functions by running the script SetObjectLevelPermissions.sql located in the "supplemental" folder of the distribution. Note that the script grants permission to user – 'advisor'. Please edit the file if you are using some other Frontline Advisor user.

11. Click OK.

12. You can now backup the database and proceed to "Creating the Monitoring Hierarchy Database" (Section 4).

Migrating Frontline Advisor Database

If upgrading from an earlier version of Frontline Advisor, the database structure can be updated using the appropriate migration script, located in the "migrations" folder of the distribution. The script name corresponds to the version being updated from. For example, When updating from FA 3.1.0, the script name is fa-database-migration-3.1-to-3.3.sql. Open the sql file in the New Query window. Select the Frontline Advisor database from the drop-down list and make sure that its name displays in the bottom of the query window (Figure 4 above). Run the script and make sure that the result is successful.

4. Creating the Monitoring Hierarchy Database

The following steps should be followed when installing a Monitoring Hierarchy Database from scratch. For instructions on updating a Monitoring Hierarchy Database from an earlier version, see "Migrating Monitoring Hierarchy Database" below.

1. Launch Microsoft SQL Server Management Studio.

2. Connect to the server where you have the new FA database already created.

3. Right-click on Databases and select New Database.
   The New Database window displays (Figure 6).
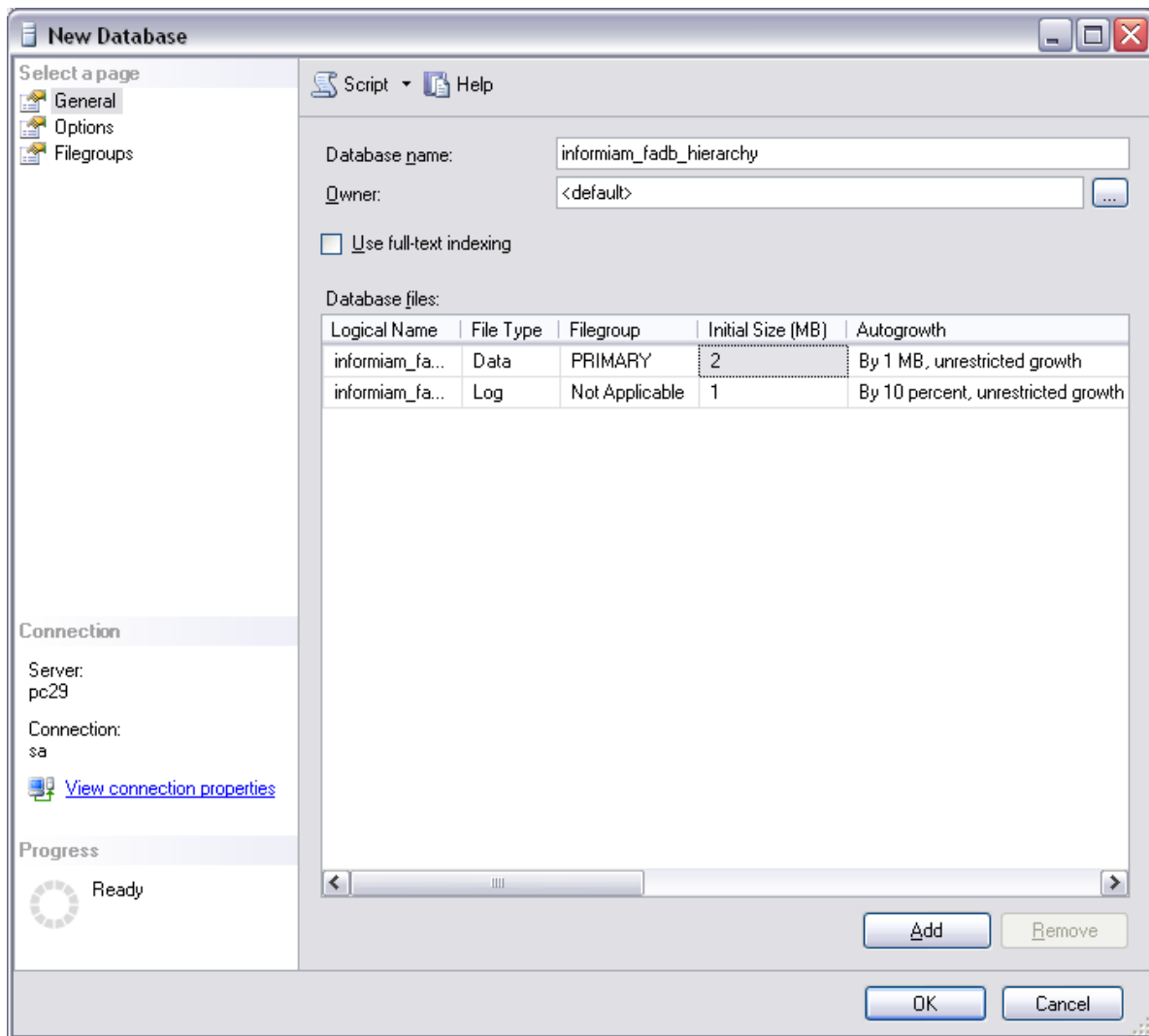
Figure 6: New Database window

4. Enter the database name. The default name for the hierarchy database is informiam_fadb_hierarchy. This name will be automatically placed into the FA DB DataSources table. If you choose to use any other name, change the DataSources entry accordingly.

5. Click Options.
   Figure 7 displays.
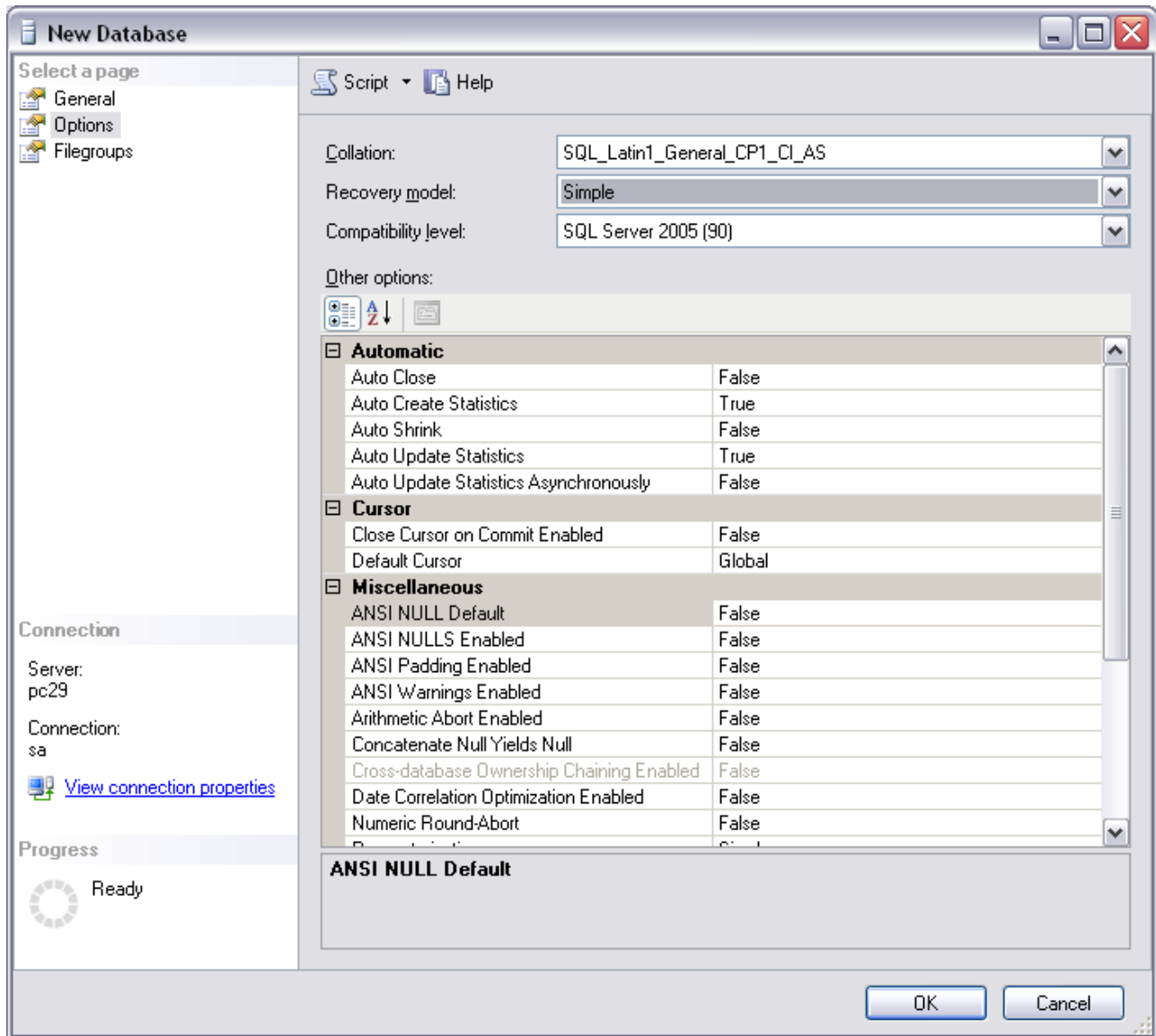
Figure 7: New Database: Recovery model

6. In the Options settings:

   a) Select SQL_Latin1_General_CP1_CI_AS for the collation.

   b) Select Simple for the recovery model.

   c) Set Auto Create Statistics and Auto Update Statistics as True.

7. Click OK.

8. Using Windows Explorer, navigate to the Frontline Advisor fa-hierarchy-mssql_xxx.sql file for your release. Run the script against the created hierarchy database. Make sure that the result is successful.

9. Your empty Monitoring Hierarchy Database is now created. See Section 6 for how to populate tables in this database.

Migrating Monitoring Hierarchy Database

If upgrading from an earlier version of Frontline Advisor, the database structure can be updated using the appropriate migration script, located in the "migrations" folder of the distribution. The script name corresponds to the version being updated from. For example, When updating from FA 3.1.0, the script name is hierarchy-migration-3.1-to-3.3.sql. Open the sql file in the New Query window. Select the monitoring hierarchy database from the drop-down list and make sure that its name displays in the bottom of the query window (Figure 4 above). Run the script and make sure that the result is successful.

5.   Installing the Frontline Advisor Server

An installer is provided that gathers configuration information and installs the Frontline Advisor server as a Windows Service.

1. Log on to the server where the installation will occur. Make sure the installer jar file can be found (Figure 8). You may need to unzip the distribution file from Informiam to do this.
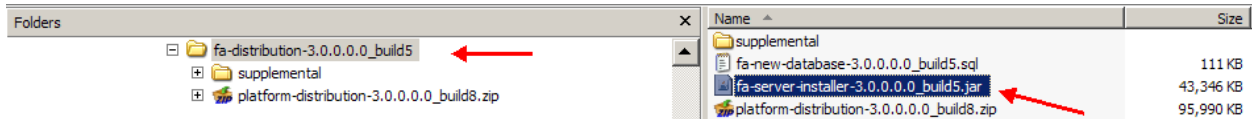
Figure 8: Frontline Advisor distribution

2. Double click on the gfa-server-installer-3.3.000.<build#>xxx.jar.
    The Frontline Advisor Installer screen displays (Figure 9)

Figure 9: Frontline Advisor Installer

3. Click Next.

    The module selection screen displays (Figure 10).
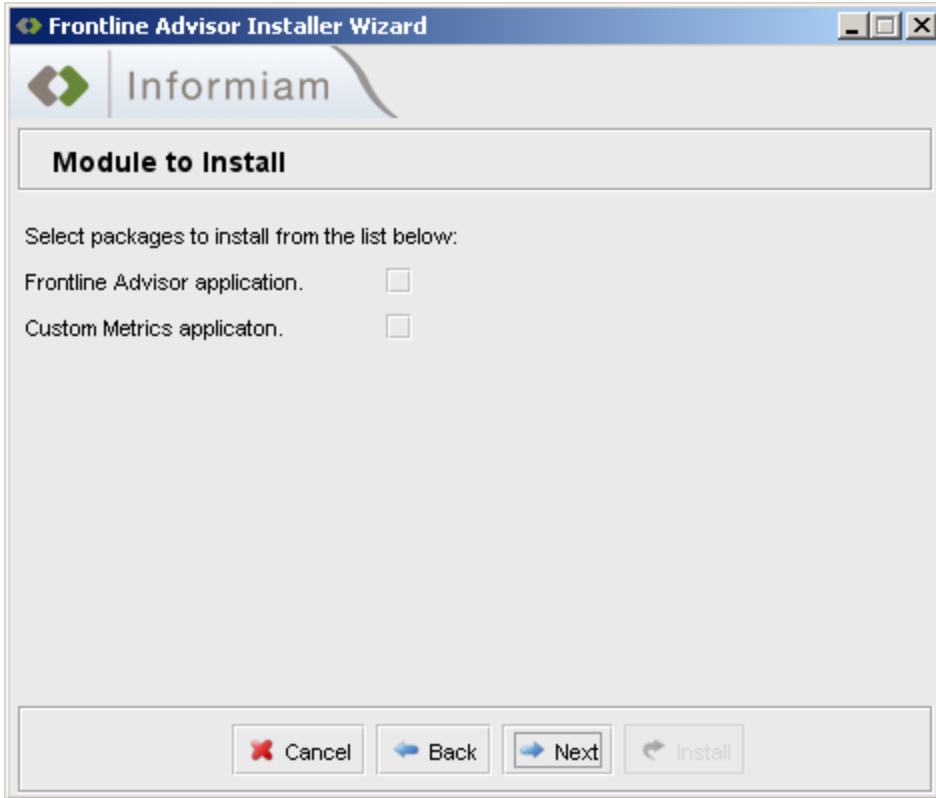
Figure 10: Frontline Advisor Destination Directory

Select the modules to install. If installing the Custom Metrics application, see "Custom Metrics Module" below.

4. Click Next.
    The Frontline Advisor Destination Directory screen displays (Figure 11).
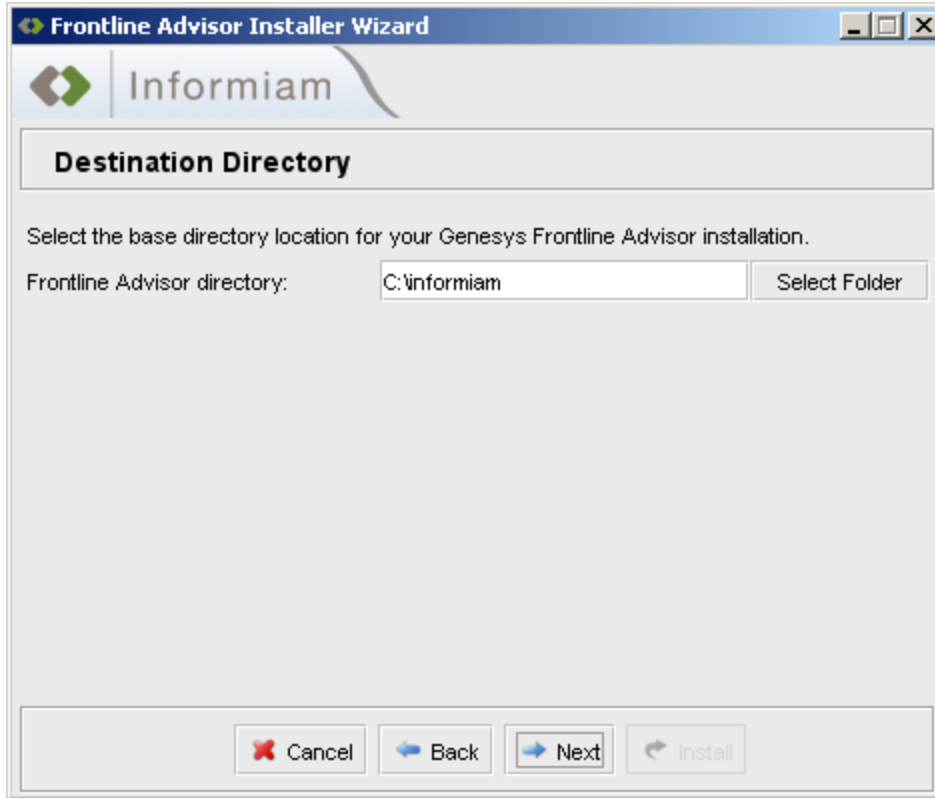
Figure 11: Frontline Advisor Destination Directory

5. Accept the default, `c:\informiam`, or install to a new location.
   The installation directory for Frontline Advisor server must be the same as the directory where the Advisors Platform 3.3.000 was installed.

6. Click Next.

The Connector Details screen displays (Figure 12). Note: this page will only appear if the option to install Frontline Advisor module was selected.
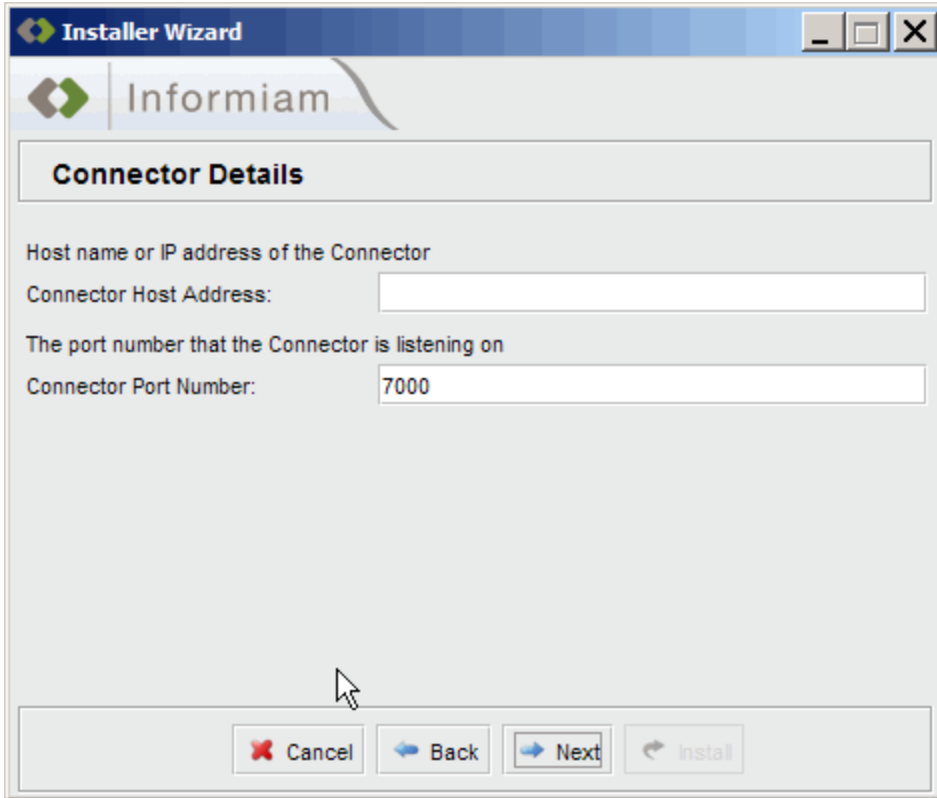
Figure 12: Connector Details

7. Provide the IP or hostname where the Genesys Adapter or Cisco Adapteris located. The port field defaults to 7000, which is the default for both Adapters.

8.   Click Next.

The Advisors Platform Database screen displays (Figure 13). Note: this page will only appear if the option to install Frontline Advisor module was selected.
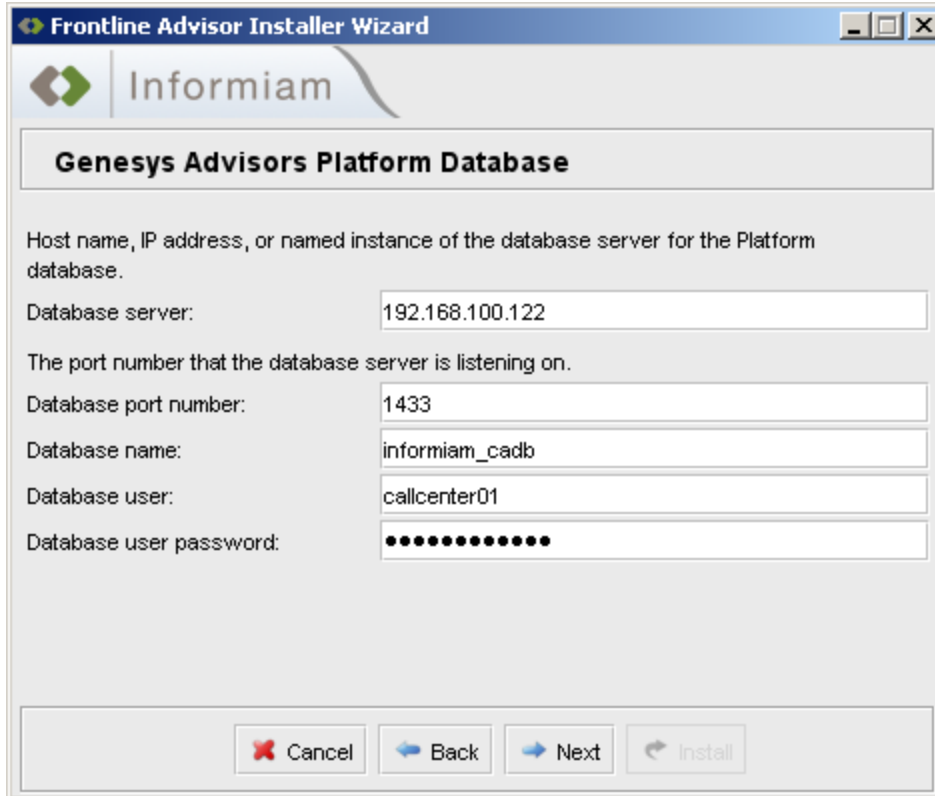
Figure 13: Advisors Platform Database

9. Enter the Advisors Platform database connectivity parameters for the already upgraded database (that is, the database must be upgraded prior to running the installer):

- Database server (machine): for example, 192.168.100.122

- Database port number: for example, 1433
  If the database server is a named instance, then omit the port number.

- Database name: for example, informiam_cadb

- Database user: for example, callcenter01

- Database user password

10. Click Next.
    The Frontline Advisor (FA) Database screen displays (Figure 14).
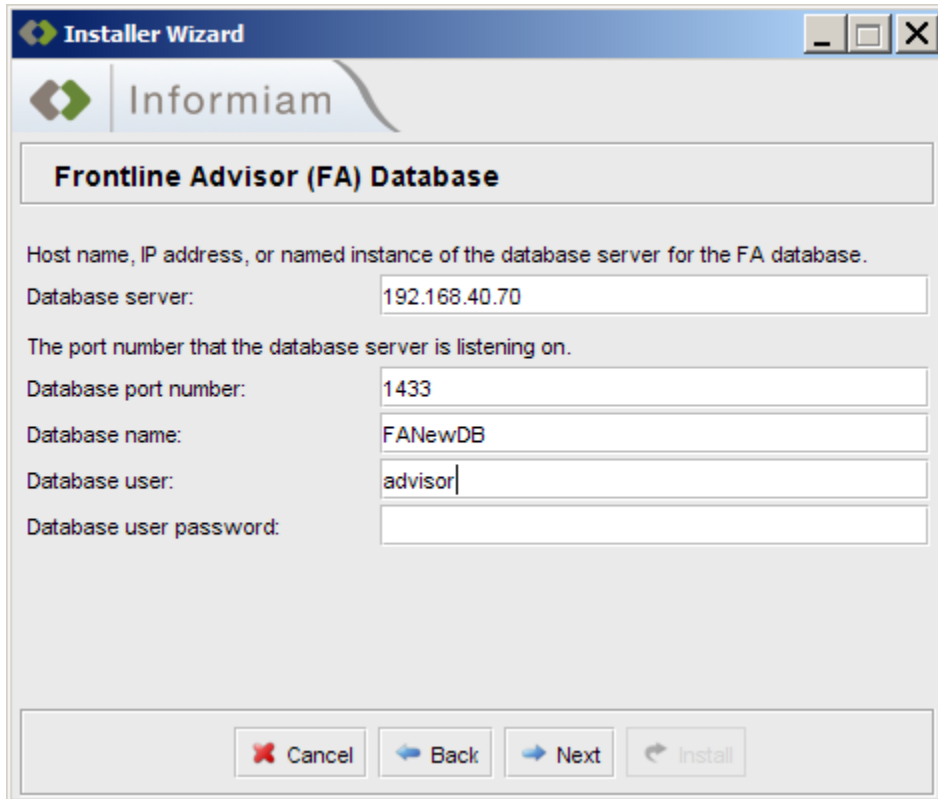
Figure 14: Frontline Advisor (FA) Database

11. Enter the Frontline Advisor database connectivity parameters for the already upgraded database (that is, the database must be upgraded prior to running the installer):

   - Database server (machine): for example, 192.168.40.70

   - Database port number: for example, 1433
     If the database server is a named instance, then omit the port number.

   - Database name: for example, informiam_fadb

   - Database user: for example, advisor

   - Database user password

12. Click Next.
    The Hierarchy Staging Database Configuration screen displays (Figure 17).
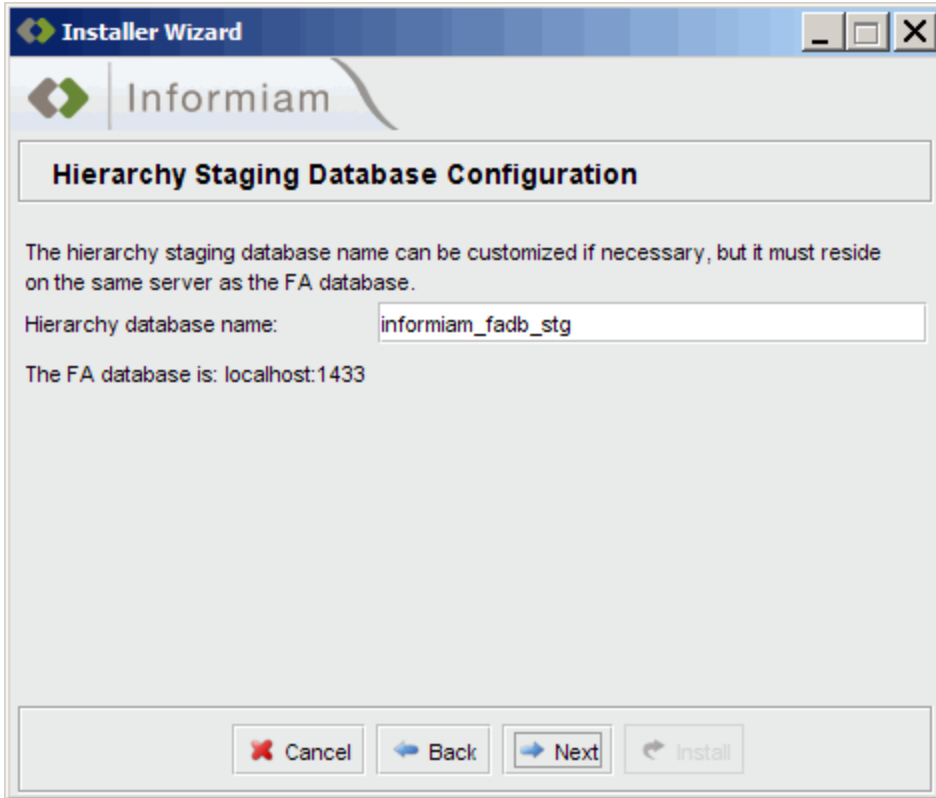
Figure 15: Hierarchy Staging Database Configuration

13. Type the Hierarchy database name, informiam_fadb_hierarchy.

14.   Click Next.
The Failure Notification Configuration screen displays (Figure 16). Note: this page will only appear if the option to install Frontline Advisor module was selected.
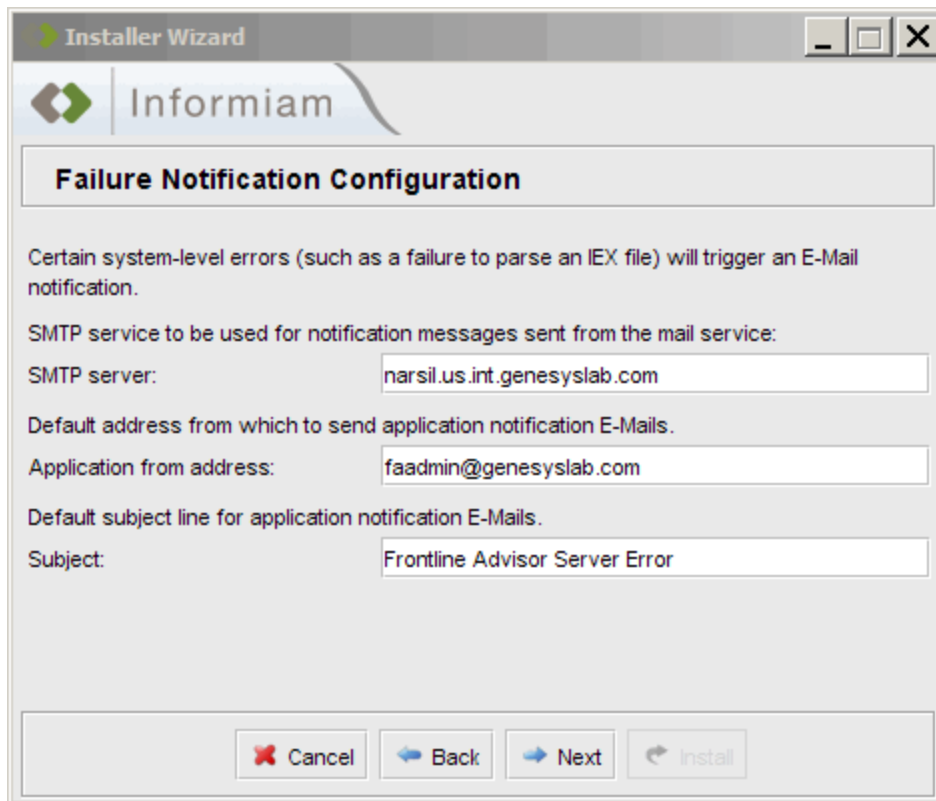
*Figure 16: Failure Notification Configuration*

15. Enter the SMTP and e-mail parameters (Figure 16):

    • SMTP server: for example, narsil.us.int.genesyslab.com

    • Application from address: for example, faadmin@genesyslab.com

    • Subject line: for example, Frontline Advisor Server Error

16. Click Next.
    The Installation Progress screen displays (Figure 17).
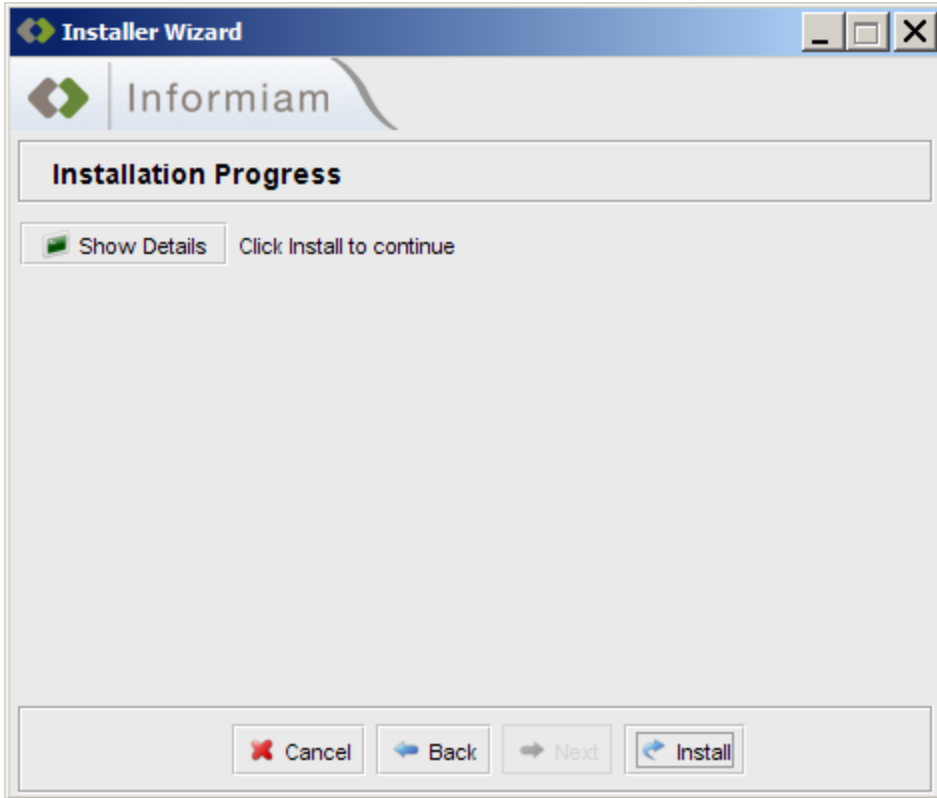
Figure 17: Installation Progress17. Click Show Details then Install and verify there are no errors during the installation. If the installation is successful, you will see a message "Build Successful" displayed.

6. Populating the Monitoring Hierarchy Database

Overview

The Frontline Advisor application loads the hierarchy data from the hierarchy database. The hierarchy database resides on the same SQL Server as the Frontline Advisor database. The default name of the hierarchy database is informiam_fadb_hierarchy. It is specified in the DataSources table of the Frontline Advisor database in the record with the SourceType = 'hierarchy'. The name of the hierarchy database can be changed if necessary.

The database with the corresponding name must be created by a DBA or a member of the services team.

The recovery model, the collation, and the user must be the same as that of the Frontline Advisor database.

The distribution will contain a separate script to create hierarchy datebase objects which must be run against the database once it is created.

The content of the hierarchy database must be prepared before the Frontline Advisor application is first started.

Import Schedule

The very first time Frontline Advisor is started, the entire Monitoring Hierarchy is imported from the source that was defined during installation. Once Frontline Advisor is running the Monitoring Hierarchy Importer is scheduled to run daily at 2:55 a.m. server time.

Loading data into the informiam_fadb_hierarchy database

Follow the sequence and rules for loading data into the informiam_fadb_hierarchy database.

1. FA_HIER_Person table

Prepare the list of people that are expected to have related data in the Frontline Advisor application, that is, managers of all levels and agents, then load the data into the FA_Hier_Person table of the hierarchy database.

- A unique enterprise-wide ID must be specified for each person. BadgeId or EmployeeId are examples of global ids.
- The format of global ids is not restricted. Global ids can contain numbers as well as characters.
- The GlobalId and LoginName must be unique within the list.
- Records that contain 'Unknown','Undefined', 'Enterprise' or any other artificial content are not acceptable.

Note that based on the first name, last name, and the e-mail pattern, the Frontline Advisor application will generate the e-mail addresses for the Advisors Platform database's Contact table. The pattern for e-mails is taken from the hierarchy record of the Frontline Advisor DataSources table.

The domain is stored in the DataSources table of Frontline Advisor.

Person		
PersonID	nvarchar(64)	A unique enterprise-wide ID assigned to the person (i.e., some employeeid or badgeid...). FA_Hier_Person table contains an enterprise-wide list of employees of all levels.
Fname	varchar(128)	First name
Lname	varchar(128)	Last name
LoginName	varchar(50)	The loginName is unique within the enterprise.

2. FA_HIER_Agent table

Prepare the list of all agents then load the data into the hierarchy FA_Hier_Agent table.

- AgentSkillId must be unique within the same call management system. AgentSkillid is the ID that displays in the real-time agent data and in the details of the calls taken by an agent. In a Cisco environment, the AgentSkillId matches the SkillTargetId field in the Agent_Real_Time table. In a Genesys environment, the AgentSkillId has the format [Tenant-Name] Employee-ID. In a single-tenant environment, the Tenant-Name for all agents is 'Resources'.
- The same person can have more than one AgentSkillId within the same call management system.

- Agents that do not belong to any team must not be present in the hierarchy database.
- If a person has a supervisor role (that is, is a team supervisor) as well as an agent role then this person must belong in the list of agents.

Agent		
AgentSkillID	varchar(500)	Call management system numeric ID assigned to an agent (i.e., SkillTargetID, ACDid, ...) Several AgentSkillIDs can be assigned to one agent identified by a unique PersonID.
PersonID	nvarchar(64)	A unique enterprise-wide ID assigned to an agent (i.e., some employeeid or badgeid...). This is a foreign key which references the FA_Hier_Person table. The FA_Hier_Person table contains an enterprise-wide list of employees at all levels.
SourceID	Int	The ID of the source related to an AgentSkillID (i.e., the data can be loaded from different call management systems. Since AgentSkillIDs can overlap in this case, a SourceID must be supplied with each AgentSkillID.

3. FA_HIER_Team table

Prepare the list of all teams then load the data into the hierarchy FA_Hier_Team table.

- TeamId must be unique within the same call management system.
- Eliminate the records like 'Unknown' or 'Undefined'. The list must contain a set of valid teams.
- Each team must have a primary supervisor.

Team		
TeamID	nvarchar(64)_	The ID of a team. TeamId is a part of the primary key. It is expected that the ids of the teams that originate from different call management systems can overlap. SourceID is used to insure each record's uniqueness.
EnterpriseName	varchar(128)	The name of a team.
PriSupervisorPersonID	nvarchar(64)	The PersonID of an employee who is a primary supervisor for the team. Each agent team can have only one primary supervisor.
SourceID	Int	The ID of the source call management system agents from which are the members of the team. SourceID is a part of the primary key.

4. FA_HIER_Agent_Team_Member table
Specify which agents are members of which teams.

Note that AgentSkillId from one call management system cannot be related to a TeamId from another call management system. The combination of TeamId and AgentSkillId must be unique within one call management system, that is, within one source. See section 2 above for the format of AgentSkillId.

Agent_Team_Member		
TeamId	nvarchar(64)	The ID of the team. AgentTeamId is a part of the primary key. It is expected that the ids of the teams that originate from the different call management systems can overlap. The SourceID is used to insure each record uniqueness.
AgentSkillId	varchar(500)	Call management system ID assigned to the agent (i.e., SkillTargetID, ACDid, ...) Several AgentSkillIDs can be assigned to one person identified by a unique PersonID.
SourceId	Int	The ID of the source related to the AgentSkillID (i.e.,the data can be loaded from different call management systems. Since AgentSkillIDs can overlap in this case a SourceID must be supplied with each AgentSkillID.

5. FA_HIER_Supervisor_Team table

Specify the list of all supervisors for each team including primary and backup supervisors.

Supervisor_Team		
TeamId	nvarchar(64)	The ID of the team. AgentTeamId is a part of the primary key. It is expected that the ids of the teams coming from the different call management systems can overlap. SourceID is used to insure each record's uniqueness.
SupervisorPersonId	nvarchar(64)	PersonID of the employee who is a primary or backup supervisor for the team. Each agent team can have only one primary supervisor and several backup supervisors. The primary supervisor PersonID is stored in the FA_Hier_Team_Table.
SourceId	int	The ID of the source call management system. SourceID is a part of the primary key.

6. FA_HIER_Supervisor_Supervisor table
Specify the hierarchy of managers.

- SupervisorPersonId and BossPersonId cannot be the same.
- A pair of SupervisorPersonId containing PersonId1 and BossPersonId containing PersonId2 cannot belong in another record where SupervisorPersonId contains PersonId2 and BossPersonId contains PersonId1.
- Both ids must reference the ids of real people in the FA_Hier_Person table.

Supervisor_Supervisor		
SupervisorPersonId	nvarchar(64)	PersonID of the supervisor
BossPersonId	nvarchar(64)	PersonID of the boss of the above supervisor

7. Starting the Frontline Advisor Service

Follow the Advisors Platform instructions to install the Windows service. Each time the service is started, the Monitoring Hierarchy Loader runs (see Section 6), so before starting the Frontline Advisor service the first time, the work in Section 4 must be performed. Start the service and refresh a few times to make sure the service stays running. Check the Platform and Frontline Advisor log files if you experience problems.

It may take several minutes to fully start Frontline Advisor, depending on the number of agents and the complexity of the hierarchy.

8. Configuring Apache Routes

Assuming Advisors Platform and Apache have been installed, locate your Apache configuration file, httpd.conf, in the section that configures 'ProxyPass' for the Advisors Platform server.

In that same section, add a new entry for Frontline Advisor, using the IP address of your installed Frontline Advisor server:

```
ProxyPass /fa/ ajp://192.168.40.234:8009/fa
```

Frontline Advisor requires a connection to the Preferences Service and Navigation Service. If an Apache route has not already been configured then add a new route to httpd.conf. The preferences service is installed with the Platform navigation service so use that servers IP or name:

```
ProxyPass /prefs-service/ ajp://<IP Address of Advisors Platform
server>:8009/prefs-service/
```

```
ProxyPass /nav-service/ ajp://<IP Address of Advisors Platform
server>:8009/nav-service/
```

9. Verifying Server Connections

Verify the Frontline Advisor Server connection

In your browser, type:

```
http://localhost:8080/fa/com.informiam.fa.admin.gwt.
AdminConsole/AdminConsole.html
```

If configured correctly and this is the first time you are logging in, the Login page displays. If this is not the first time you are logging in, the Administration page displays. You can exit from the Internet Explorer browser.
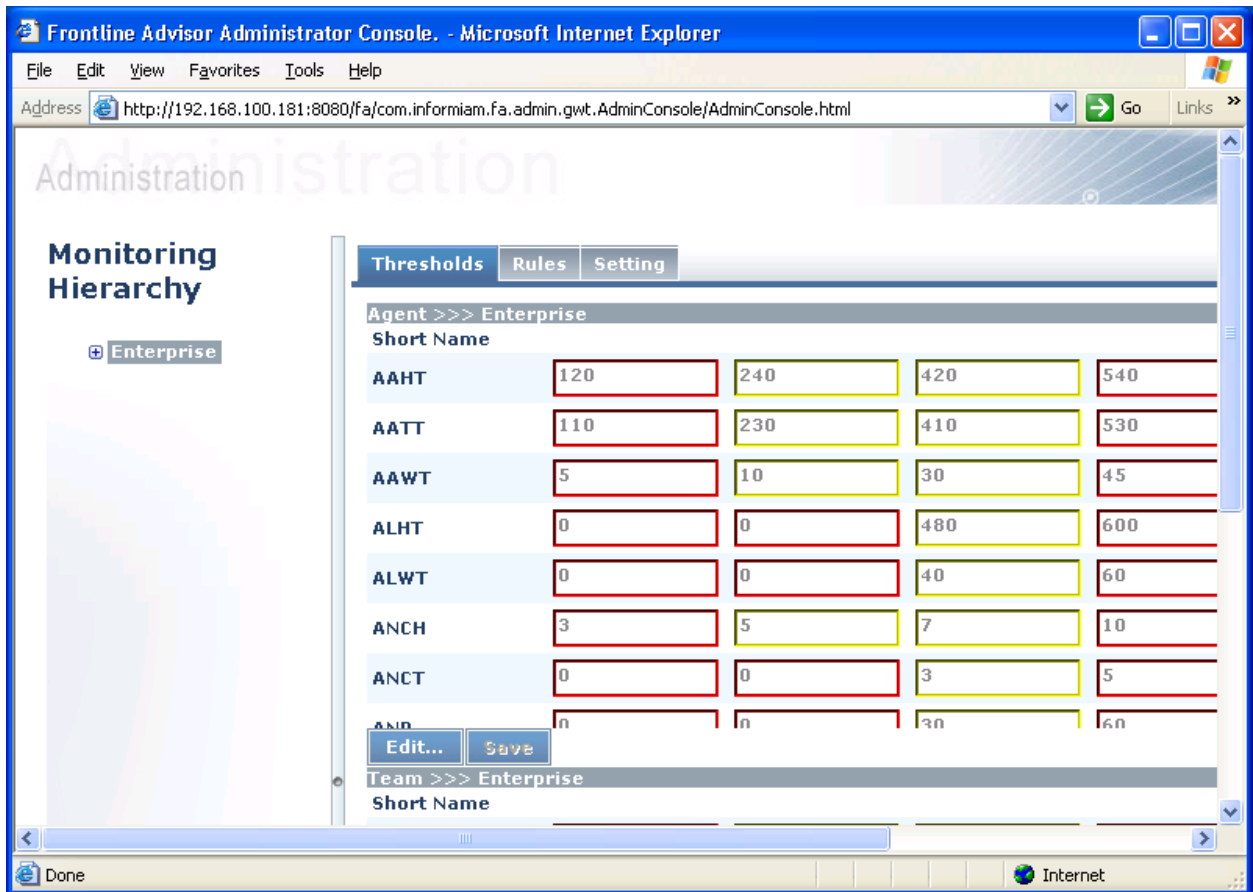

Figure 18: Login page

Verify Apache Routing

Use a normal Web browser to connect directly to the Apache server, log in and check the site. Use a URL that contains the host or IP address (and optionally the port if not on port 80) of the Apache server.

If configured correctly, the Login page displays. You can exit from the Internet Explorer browser.

Verify the Informiam Browser Connection

To check the Frontline Advisor application, launch the Informiam Browser, log in, and check the site.

Integrating External Links

To configure external links on the Manager Console and Agent Console, change the contents of the property file named `FrontlineAdvisor.properties` which is located in the conf subdirectory of the Frontline Advisor installation directory .

In addition to setting the URL links, additional parameters can optionally be used:

- **user**
- **moduleId**
- **teamId**
- **primarySupervisorPersonId**
- **agentPersonId**
- **errorCode**

This is the acceptable link-in URL for Informian Browser.

- informiam:///?user=[user_login]&module=FAAgentConsole
- informiam:///?user=[user_login]&module=FASupervisorConsole
- informiam:///?user=[user_login]&module=FAAdmin

The module is the code value of each module in the Module table of the Advisors Platform database, which can be configured through the Platform Administration Workbench. Those values might be passed out to an external application by the Link Out URL parameters.

Changes to these URL's requires a restart of Frontline Advisor to take a effect.

Currently the user must enter a password to log in to the Informian Browser by link-in URLs.

This is an example of an acceptable Link Out URL that follows the URL template in the url.properties file:

```
http://somehost?user&moduleId&teamId&primarySupervisor
PersonId&agentPersonId&errorCode
```

- **user**: filled in by the server when the user is authenticated
- **moduleId**: retrieved from the EA database (MODULE table) based on the application deployment URL (e.g., /fa/SupervisorConsole) provided by the client requesting the Link Out URL
- **teamId**: filled in by the client
- **primarySupervisorPersonId**: filled in by the client
- **agentPersonId**: filled in by the client

10. Additional Items

Changing the Frontline Advisor Module URLs

The installer makes the necessary configurations for the Informiam Browser to connect to the Frontline Advisor modules. If you need to change these URLs, use a custom SQL query but do so at your own risk.

Configuring Memory Allocation

To configure memory allocation, see *Changing the memory allocation to the documents* in the InformiamPlatform_InstallationGuide_3.0.0GA.pdf.

Truncating the Violations Archive Table

The DBA on the client site must put a job in place that truncates the FA_Violations_Archive table. This truncation should take place once every n-number of days (the 'n' depends on customer requirements).

Changing the Values at the Enterprise Node

The rules and thresholds are defined but disabled by default at the Enterprise level and cannot be removed from that level. Once the application starts up, these values can be changed and overridden at lower levels of the hierarchy for more fine-grained control.

Appendix A.   Automated Installation Options

In addition to installing Frontline Advisor using the graphical installer ("normal mode"), there are two additional installations modes which permit some degree of automation: "semi-silent" and "silent". Details of the installation modes, as well as instructions on their use and their limitations, can be found in the *Advisors_Platform_InstallationGuide_3.3.000GA.pdf*. The command for invoking the installer in silent mode is

```
java –jar gfa-installer-<version #>.jar swing-auto
```

Appendix B.　　Custom Metrics Module

Custom metrics are supported via a separate Geronimo-deployed sister application, which can be selected as an installation option on the Frontline Advisor installer. Custom metrics are described in a set of configuration tables in the FA hierarchy database, with agent-level source metrics provided by an external application and aggregated by the Custom Metrics module.

B 1.　　Installation

The Frontline Advisor Installer has an option to install the Custom Metrics module, which can be deployed on the same Geronimo instance as FA itself, or on a separate machine. If deployed separately, when prompted for the location of the FA database and associated hierarchy database, the same connection parameters must be supplied for both modules. After the Custom Metrics module is installed, a new record will be added to the FA_Datasources table in the FA database, with the following properties:

- SourceName – this will be the same as the hierarchy database name
- SourceType – 'customdata'
- SourceActive – True

If "SourceActive" is later changed to 'False', the CMM will be disabled

B 2.　　Meta-Data Configuration

There are three tables in the hierarchy database which are involved in the definition and recording of custom metrics.

B 2.1 Custom Data

The FA_HIER_CustomData table is where the raw agent-level data is imported by an external process, which the CMM will use to aggregate into custom metric values. By default, three columns will be defined:

- AgentSkillId
- SourceId
- UpdateDateTime

AgentSkillId and SourceId identify the agent for whom the data applies. UpdateDateTime is used to track the last time any custom data for an agent changed. In addition to these default columns, additional columns must be added corresponding to the raw metrics that are used in calculating custom metrics. These columns should have a datatype of 'float' (only numeric metrics are supported).

B 2.2 Custom Metric Definitions

Custom metrics are defined in the FA_HIER_Metric table. This data is read on the same schedule as the hierarchy data (at startup and once per day thereafter). The following fields are configured for each metric:

- MetricPatternNum
- MetricName

- MetricDisplayName
- MetricDescription
- MetricRollupType
- MetricBaseFormula
- UpdateDateTime

MetricPatternNum, MetricName, MetricDisplayName, and MetricDescription are text fields that identify and describe the metric. MetricName must not collide with any default FA metrics (nch, aht, etc). It should be a short identifier, such as an acronym. MetricDisplayName is a longer descriptor that will often show up in a tooltip on the Dashboards.
MetricBaseFormula describes how raw data in FA_HIER_CustomData is combined to determine custom metric values at the agent level. The format is a formula that contains:

- operands: literal numerical values or column names from FA_HIER_CustomData
- operators: any of the following: +,-,/,*

For example, the metric 'TotalRevenue' might be defined as 'RevenuePerCall * CallVolume', where these two operands match the names of columns in FA_HIER_CustomData. If any formula validation fails these constraints, the insert of the whole batch containing it will be rolled back.
MetricRollupType specifies how the agent-level custom metric value is aggregated up to teams and through the hierarchy. The following values are supported: SUM, MIN, MAX.
UpdateDateTime is updated each time a metric definition changes

B 2.2 Custom Metric Thresholds

Thresholds for custom metrics may be optionally defined for each custom metric, once at the agent level, and/or at the team level. The following properties in FA_HIER_DefaultThreshold describe a threshold:

- MetricName
- ThresholdLevel
- AcceptableLow
- AcceptableHigh
- CriticalLow
- CriticalHigh
- UpdateDateTime

MetricName identifies the metric.
AcceptableLow, AcceptableHigh, CriticalLow, and CriticalHigh describe the bounds for the threshold, exactly as in the FA_Thresholds table.
ThresholdLevel is either 2 for team-level thresholds, or 3 for agent-level thresholds
UpateDateTime is updated each time a threshold definition changes.

B 3. Run Time Behavior

Thresholds defined in the FA_HIER_DefaultThreshold table will be imported into the list of predefined metric thresholds when FA starts up. They will be defined at the Enterprise level, and

disabled by default. The FA Administration console can then be used to modify and override these thresholds normally. Note that subsequent changes to the values of a record in FA_HIER_DefaultThreshold are not migrated to the FA database. There is no support for defining Rules against custom metrics.

As noted above, updated meta-data configuration (in FA_HIER_Metric and FA_HIER_DefaultThreshold) will be refreshed on the same schedule as the hierarchy data. Since the data contained in the custom metrics portion of the schema is interdependent, it's critically important to restart Fronline Advisor (both the FA module and Custom Metrics module) if any changes in the meta data is likely to cause an inconsistency. For example, changing a metric definition or the name of a raw metric column in FA_HIER_CustomData would be examples of changes that would require a restart.

Custom metrics are retrieved along with other performance-related metrics and are displayed in both FA consoles. They will also appear in the column choosers in the performance metrics section.