CAT Authentication Server Administrator User Guide

Version 4.8.X

Updated on the 24nd January 2013

This document is constantly updated. We encourage our customers to review the document and send us comments about its content and usability. Thank you.

It is all about security

Contents

Introduction to Cellular Authentication Token

One Time Password (OTP) is an established methodology for Strong Authentication. The methodology has been around for years protecting access to remote servers and services. During the last few years the industry changed. While remote and internal servers required the security for the few, the Internet services requires security for the masses.

Today, the OTP hardware token is still used for protecting Servers, Services and network applications. The implementation of the OTP with hardware tokens has two major drawbacks:

1. **Massive deployment.** When an organization is providing secured services to large number of customers, located locally or distributed worldwide, the task of deploying the hardware tokens is huge and costly. The customers could be anonymous (like in the case of Amazon customers or ICQ users) or they could be known to the service provider (like in Internet Banking). Those anonymous customers require the same level of security, but the service provider will not buy, package and send a hardware token to an anonymous customer.

2. **Multiple passwords.** Each hardware token is used to protect only one account/site. A user that is using a number of secured accounts has to take with him everywhere a chain of hardware tokens. This is not practical in today's growing awareness for security where every web site is inclined to provide secure services. In the near future all the banks will be forced by regulations to provide TFA OTP security level to their customers. Just imagine a customer that has more than one account.

Using the cellular device instead of a proprietary hardware is the practical solution. Most people who use Internet are lost without their cellular. They will not forget it and carry it anywhere. Those people are familiar with the usage of the Cellular and do not have to be educated or introduced to new technology.

- The **CAT** (Cellular Authentication Token) **is** a soft token. It is software that runs on Cellulars. It does not need communication and does not use SMS. It is installed on the Cellular like a Cellular game or ring tone.
- The **CAT** is easy to deploy and can manage any number of accounts/sites on the same device.
- The **CAT** Authentication Server is a comprehensive management system for the organization administrator. It is intuitive and easy to use.
- The system includes Identity Management, Active Directory synchronization and supports Radius enabled devices/software such as Citrix, Check Point, Cisco, MS ISA etc. . It integrates into Microsoft environments and can also be part of a Unix/Linux type network.
- The **CAT** has an open API that makes it easy to customize/integrate with other products and Internet active pages.
- The **CAT** is Secured, Deployable and Affordable solution for enterprises of all sizes providing OTP Strong Authentication for both Intranet and Internet.

The CAT was developed by Mega AS Consulting Ltd and the IP is protected by law and patents.

Chapter 1 – Welcome to CAT Authentication Server

What is CAT Authentication Server (CAT AS)

The CAT Authentication Server (CAT AS) is a Windows application that runs on an enterprise Server.

With the CAT AS you can:

- Manage the users accessing the server
- Manage the Authentication services
- Produce system reports
- Customize connection to Authentication clients

The CAT AS is made of the following modules:

- CAT Database (Using MS SQL Server or MySQL)
- CAT Management System (**CAT MS**)
- CAT Radius Server
- CAT Active Directory Sync
- CAT Internet Queries
- CAT API
- CAT API Web Services
- CAT Monitor
- CAT Deployment Utilities

Figure 1.1 System modules

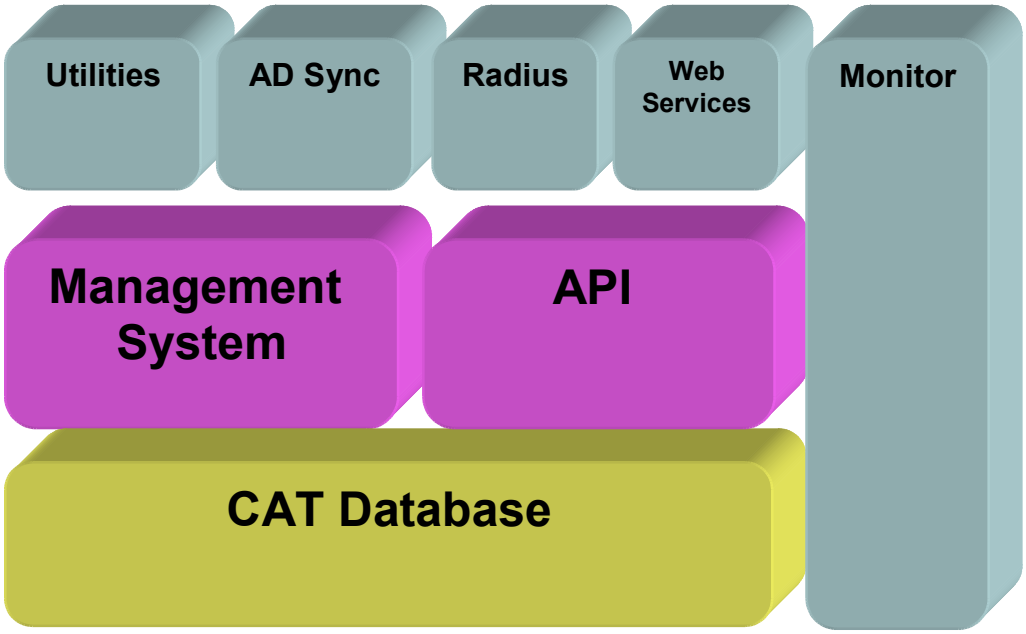
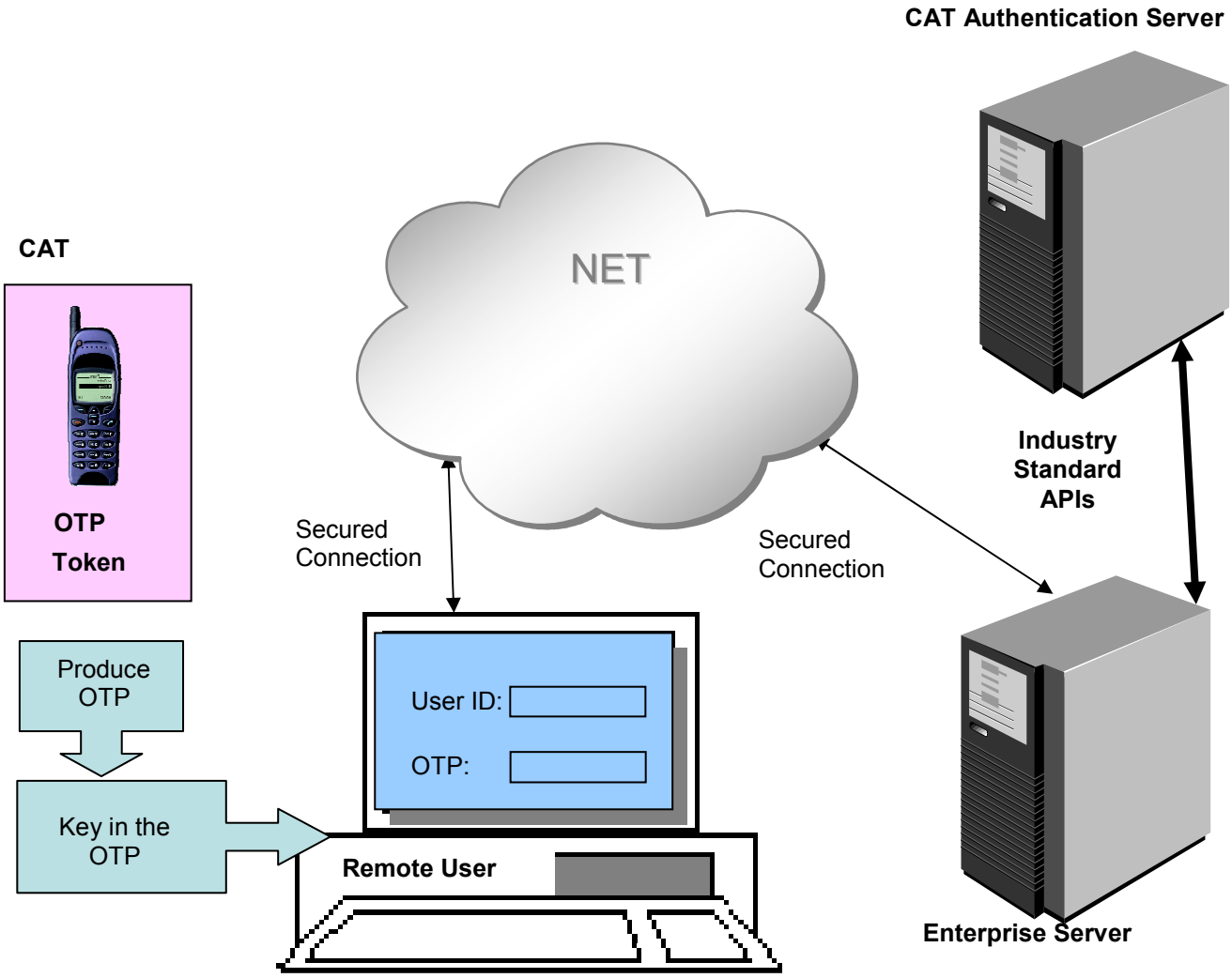


Figure 1.2 CAT Authentication System Environment



The CAT Authentication Server can be installed on the enterprise server or on another server on the Intranet or Internet.

Using this Guide

This guide shows you how to perform tasks in the CAT Authentication Server. The chapters where arranged in the logical order of the tasks to be performed.

ABBREVIATIONS AND ACRONYMS

API – Application Programming Interface
CAT – Cellular Authentication Token
CAT AS – CAT Authentication server
CAT MS – CAT Management System

Updates to this Guide

Updates to this guide can be found at the Mega AS Consulting Ltd site: www.megaas.com in the Downloads >> CAT User Guides page.

Getting Help

For technical assistance you can Email the support team: support@megaas.com

For urgent support enter Mega AS site and phone your local distributor.

Chapter 2 – Installing the CAT Authentication System

In this chapter we will go Step by Step through the Installation stages.

Requirements

CAT Authentication Server

- Windows XP Professional or 20XX Server 32B / 64B + current SP
- 100 Mb free
- Dual Core 2 MHz
- MS .Net Framework 3.5 + 4.0 (The system will try to install if unavailable)
- Legacy database (MS SQL Server, MySQL)

CAT AS API Service

Optional – used for local customization and is required for sending SMS content such as SMS OTP and/or CAT download URL.

- Installed on the same server as the CAT Authentication Server
- For sending SMS it is required to have Internet access and an SMS provider. Mega AS can provide SMS services. Contact sales@megaas.com for further information and prices.
- IIS installed (In case of 64B Server – enable 32B applications for the default pool)
- Permissions settings for Anonymous and Network Services / IIS Users settings in the database.

Preparations

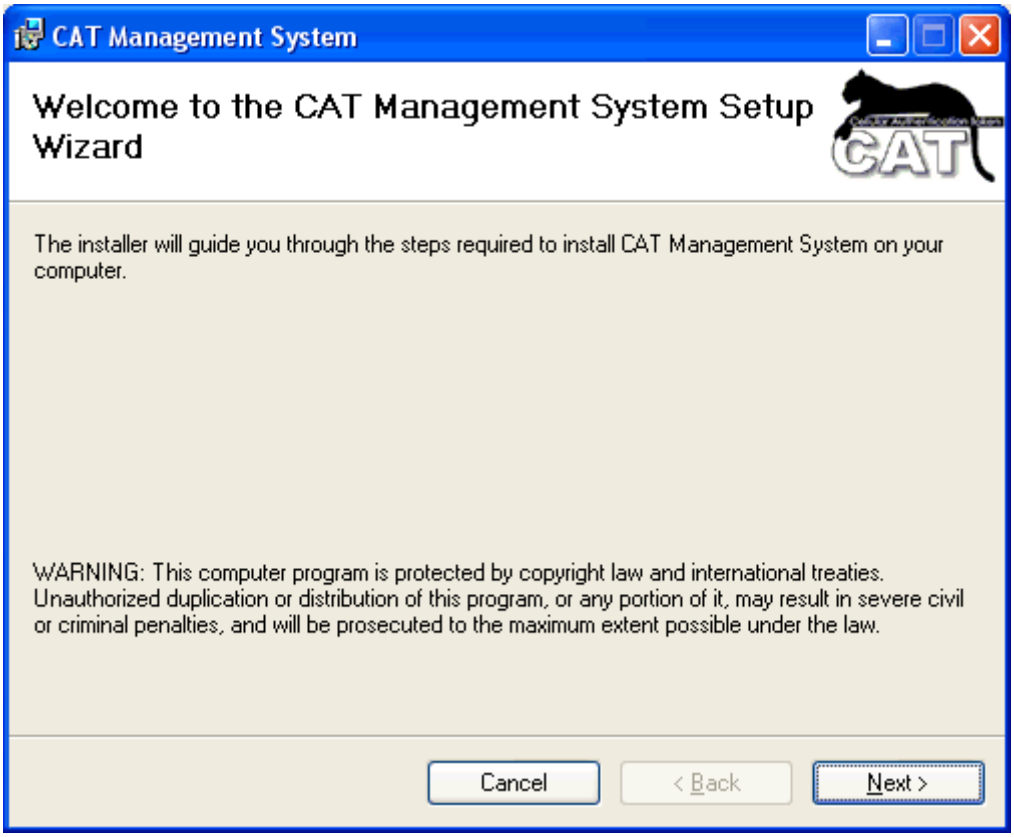
Tick	Item
	Select the database to be used. CAT MS Supports the following Databases ▪ MS Access (For demonstrating only. Not for operational site) ▪ MS SQL Server (Any version including the free Express versions) ▪ MySQL CATDB.mdb is provided with the system and can be found in the installation folder after installation. Other Databases have to be installed prior to CAT MS installation. Next you'll need to create the required tables in the Database by executing the provided SQL Scripts
	Check that you can define a DSN for the selected Database. MySQL and SQL Server may require ODBC Drivers to be installed

	Have the Database administrator ID and Password at hand
	Make sure you have Administrator privileges on the installation Server
	If you are using a Radius authentication, you may need to make changes to your Firewall to allow incoming and outgoing IPs.
	Have your company CAT Key ready. The Key dictates the number of allowed users
	Optional - API Web Services
	If you are installing the CAT Web Services check that your CAT Authentication Server is IIS enabled and that you can set a Web Service based on MS Framework 3.5 + 4.0. It is a 32B service and in case of a 64B host you need to make sure the IIS enable running 32B applications.
	You'll need a legacy database access from the enterprise Web Server such as MS SQL Server or MySQL
	For sending OTP via SMS check that you have an SMS provider. You can get an SMS account from Mega AS (conditions apply). Check with Mega AS Sales for details.
	For sending OTP via Email, you'll need and SMTP server
	For sending SMS or Emails content you may need access to the internet

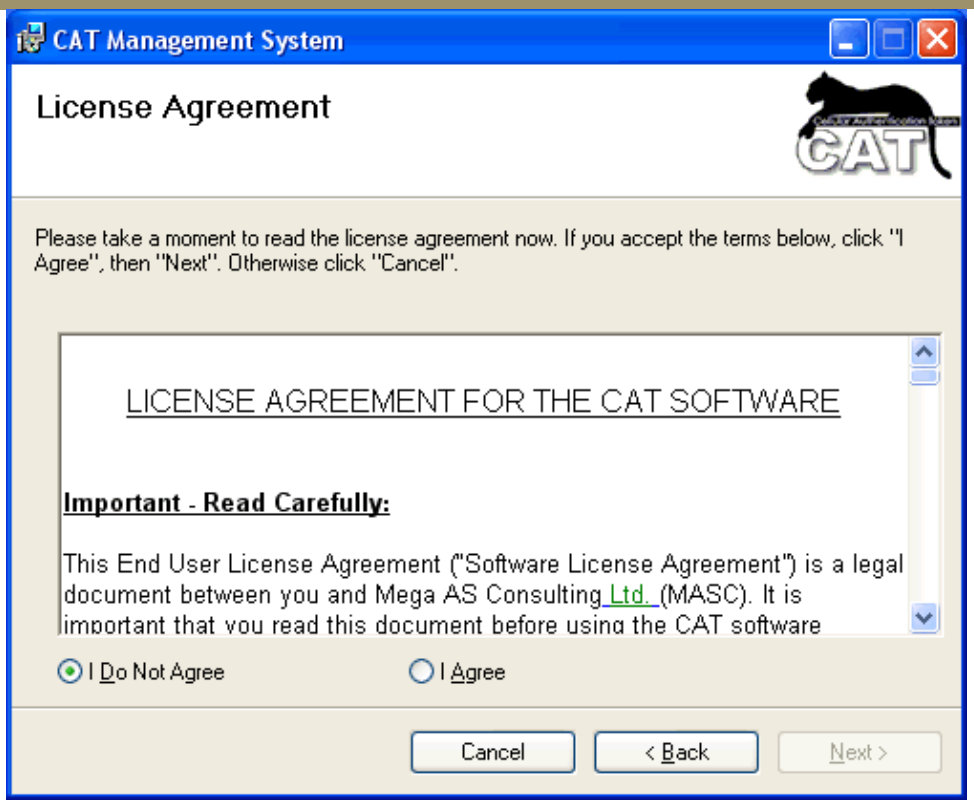
Step by Step

Installing the CAT MS

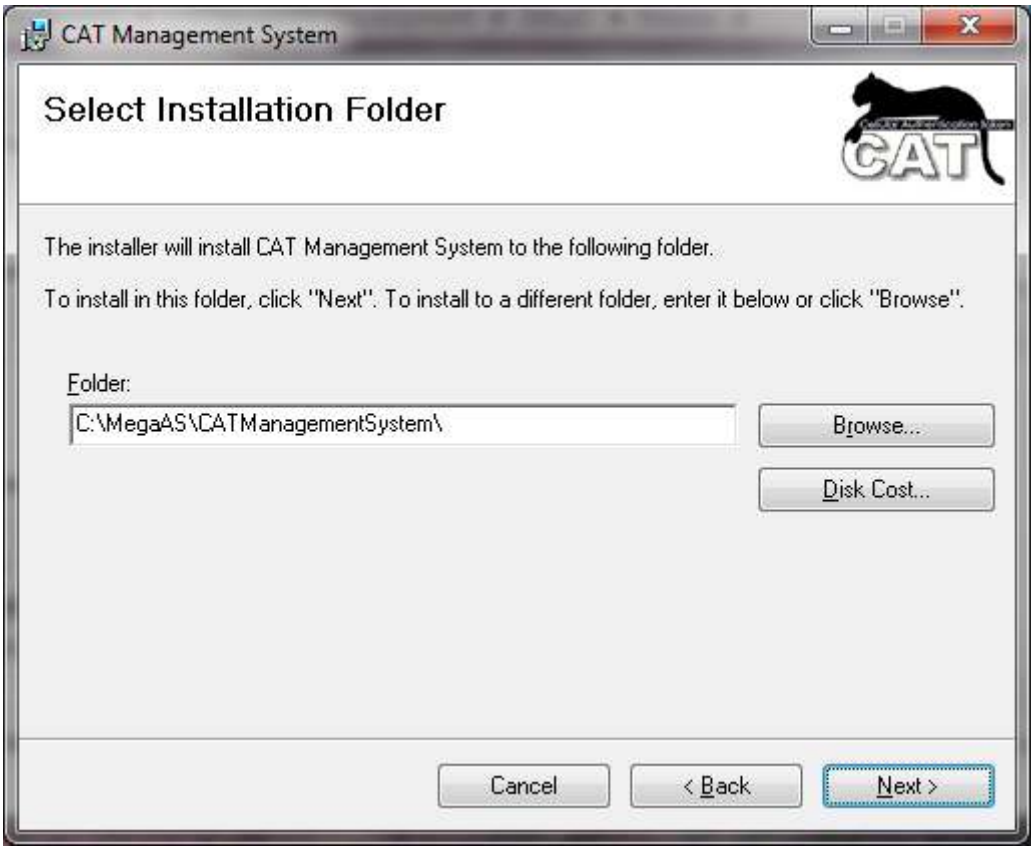
- Insert the installation CD, run the Setup.exe and follow the setup process.



Press Next to continue

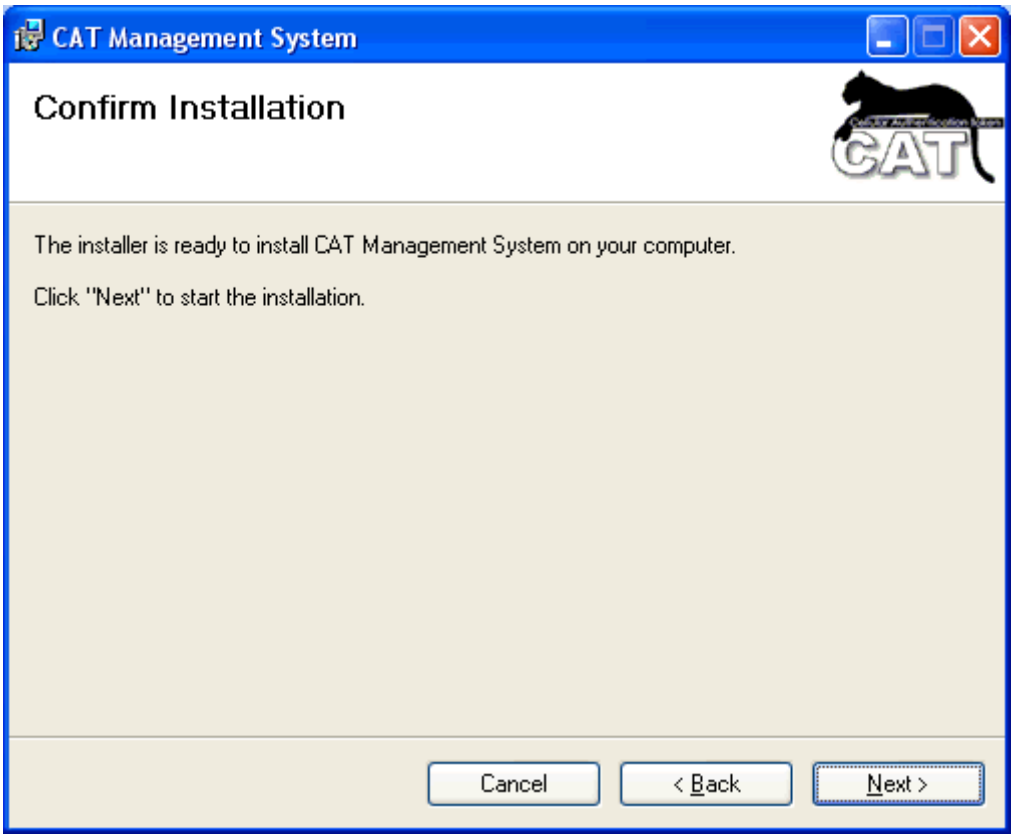


Read the License Agreement. By selecting the I Agree button you accept the agreement.
Once the agreement is accepted, you will be able to continue the installation.
Press Next to continue.



The default installation folder is at: C:\MegaAS\CATManagementSystem
You can change the default. In case that you do, please make sure that the new path does not contain special characters or blanks.

Press Next to continue.



Press Next and wait for the installation process to finish successfully.

Initializing the CAT MS

This step is done once - when you start the CAT MS the first time.
By the end of this step, you'll have the management system running and ready to add users.

The Installation adds a shortcut Icon to the Windows Desktop  .
To start the CAT MS double click on the icon.

The CAT Splash window will welcome you.

Press the Continue button.

Initiation

The CAT MS will take you through the 4 steps of initiating the system.
You'll be able to see where you are at the Application Tree on the left.

If you stop the initiation at any stage, some of the entries will be retained and the next time you start the CAT MS again, the system will take you again through the different stages.

Until the initiation is successfully completed the system is not operational.

Initiation – Step 1

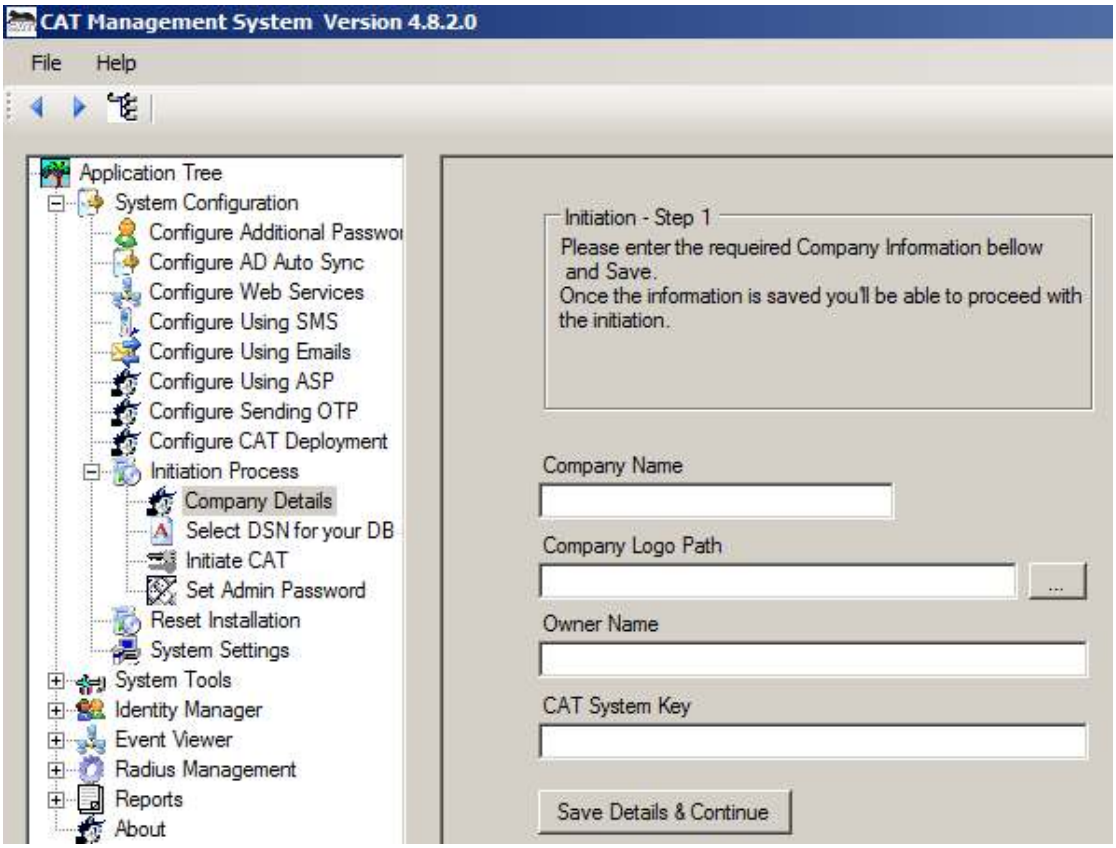
At this stage you are required to enter basic information about the installation:

Company Name – is a required field. Enter your company name.

Company Logo Path – is optional and can be selected. If you select a valid picture file, the Logo will be presented. This field is for future use.

Administrator Name – is a required field. Please enter the Administrator name.

CAT System Key – is a required field. You can get a valid key from Mega AS Ltd or its distributors at your area.



Initiation – Step 2

At this stage you are defining the access to the CAT MS database.

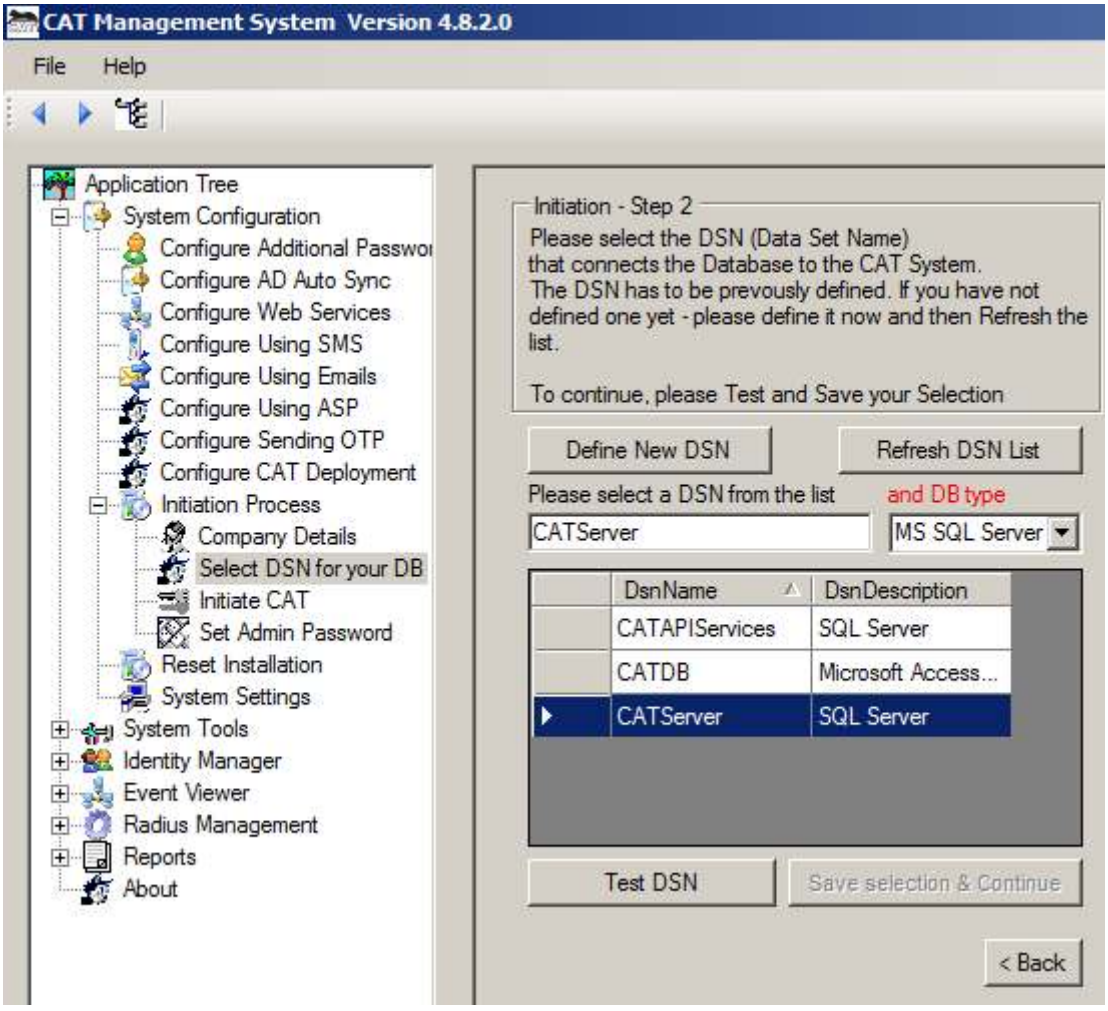
CAT MS supports 3 Databases types:

- MS Access. The CAT MS installation adds a default MS Access database to the installation folder. The database name is: CATDB.mdb **For security and stability it is recommended to use the following data bases**:
- MS SQL Server Database – for any number of users.
- MySQL Database – for any number of users.
- Other databases can be added to the list. Get in touch with Mega AS Support team.

When you use a Database **other** than the default MS Access, you need to create the CATDB Database. You can find the SQL Scripts for the appropriate Database in the SQL Scripts sub folder of the installation folder. Check Using legacy Server Databases.

When the database is ready you need to define a DSN. As a default the system will create a DSN named CATDB connecting to the CATDB.mdb database. If a DSN of the same name already exists the system will create a DSN by the name: CATDBn where n is the first available number.

You can open the DSN utility by selecting the Define DSN to Database option under **Initiation Process**, or you'll find the utility at the Windows Administrator Tools window.



After you have completed creating the DSN, press the **Refresh DSN List** button and select the DSN at the DSN List. Next, **click Test DSN** to verify the DSN and Database tables.

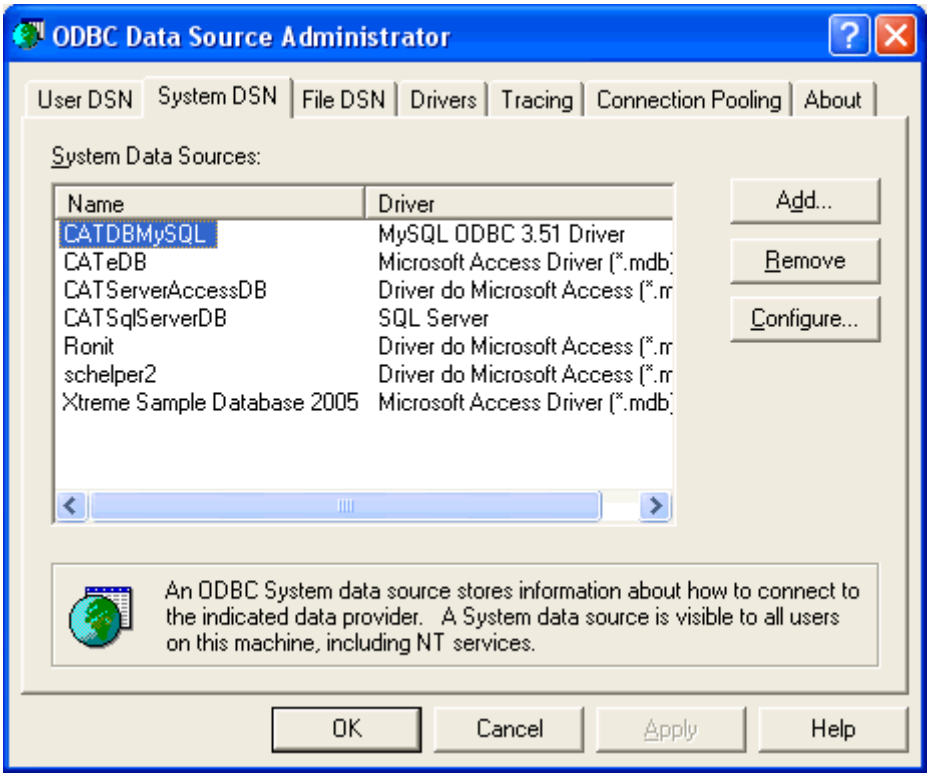
If the verification is successful you can proceed to the next step by pressing **Save selection & Continue** button.

Creating a DSN

A DSN or Data Source Name – is an ODBC Connection string managed by the Windows system and defines the necessary parameters to access a specific database.

This utility is part of the Windows Administrator Tools window.
To open the utility on a 32 B Windows:

Press Start ➔ Settings ➔ Control Panel ➔ Administrative Tools ➔ Data Sources (ODBC)



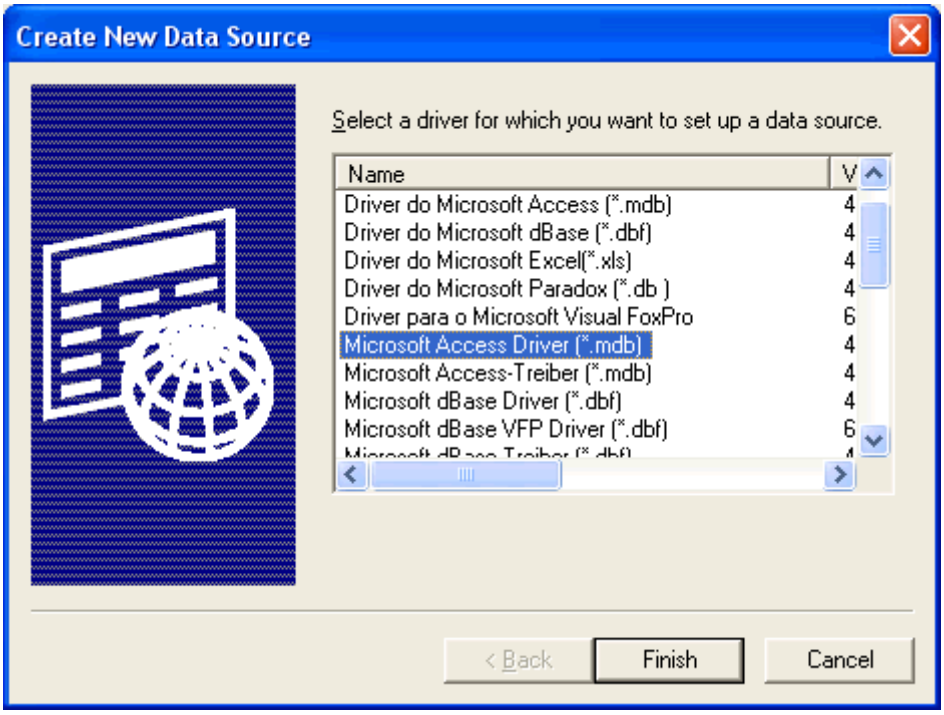
Select the System DSN tab.

You can see the existing DSN names. If this is the first time you are using the utility, then the list will be empty.

In this example we will show how to define a new DSN to the default CATDB.mdb file.

Notice – on a Windows 64B version you have to make sure you define a 32B DSN. To open the 32B version of the ODBC DSC manager open: C:\Windows\SysWOW64\odbcad32.exe

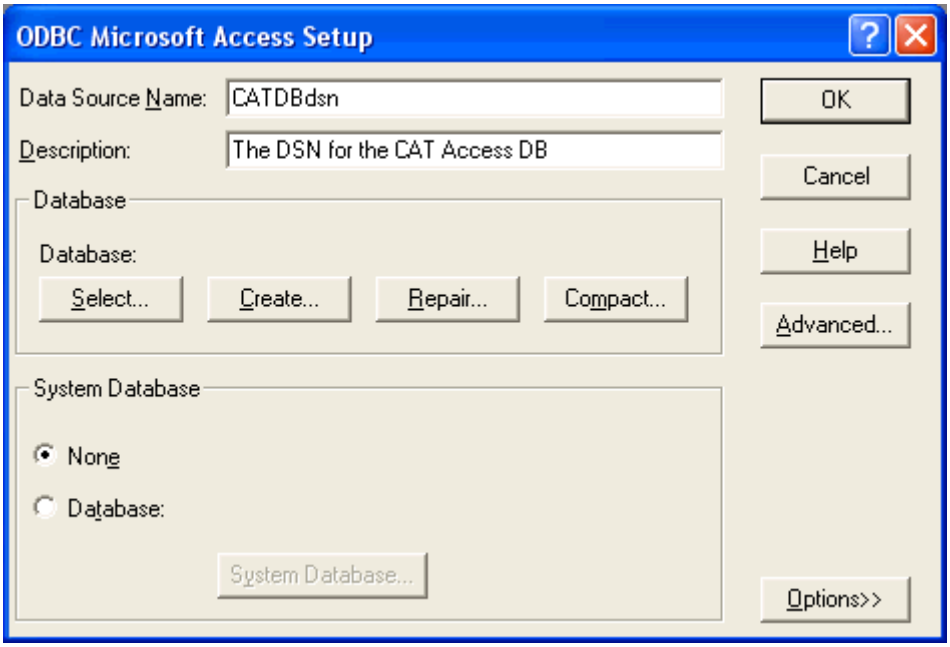
Press Add to continue.



Pressing Add opens the above window with list of available drivers to specific databases.

Please select the MS Access driver. If you can't find the above entry, you'll need to download from the Internet the latest MS Data Access (MDAC) package and install it.

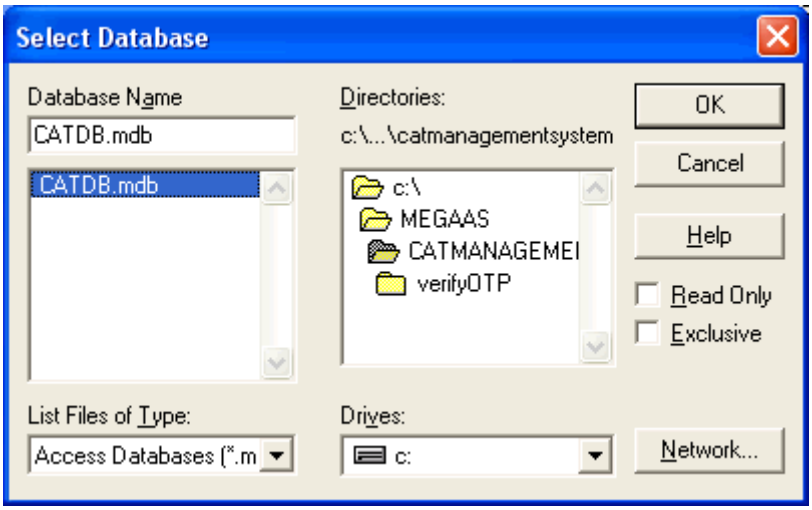
Press Finish to continue.



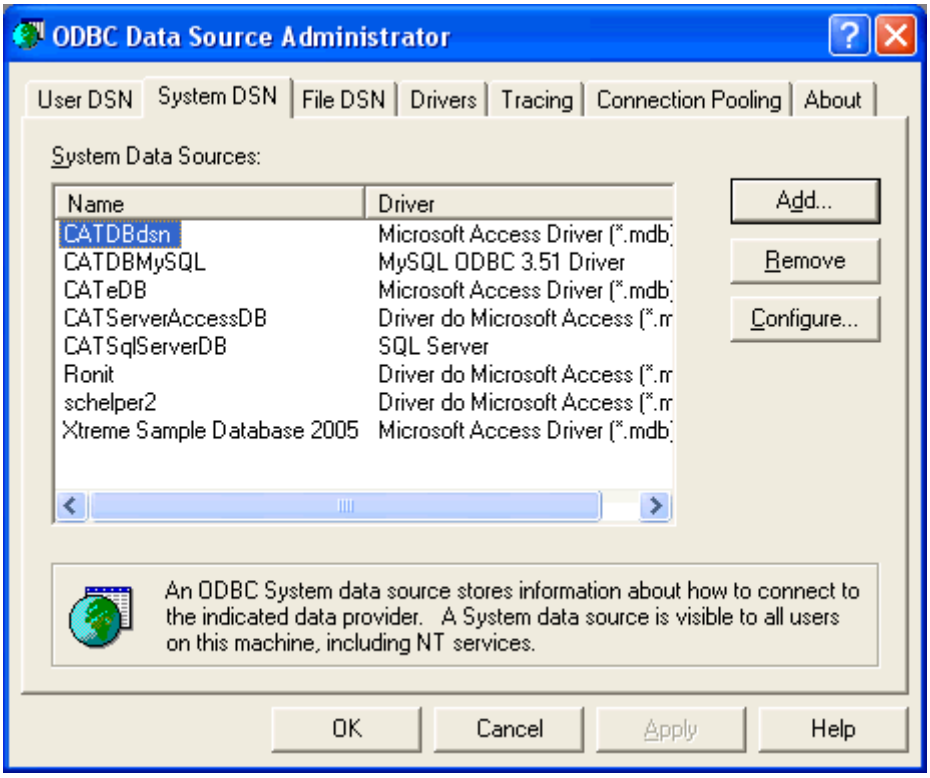
In the above window the Data Source is a required field. Please enter any name that you'd like to use. Make sure not to use special characters or blanks.

The Description is optional.

Press the Select button to continue.



Select the CATDB.mdb at your Installation path and press OK to continue.



Now you can see the new DSN in the System Data sources list.

Press OK to close the Windows

Refresh DSN List in the CAT MS Initiation Step 2 Windows and continue.

Initiation – Step 3

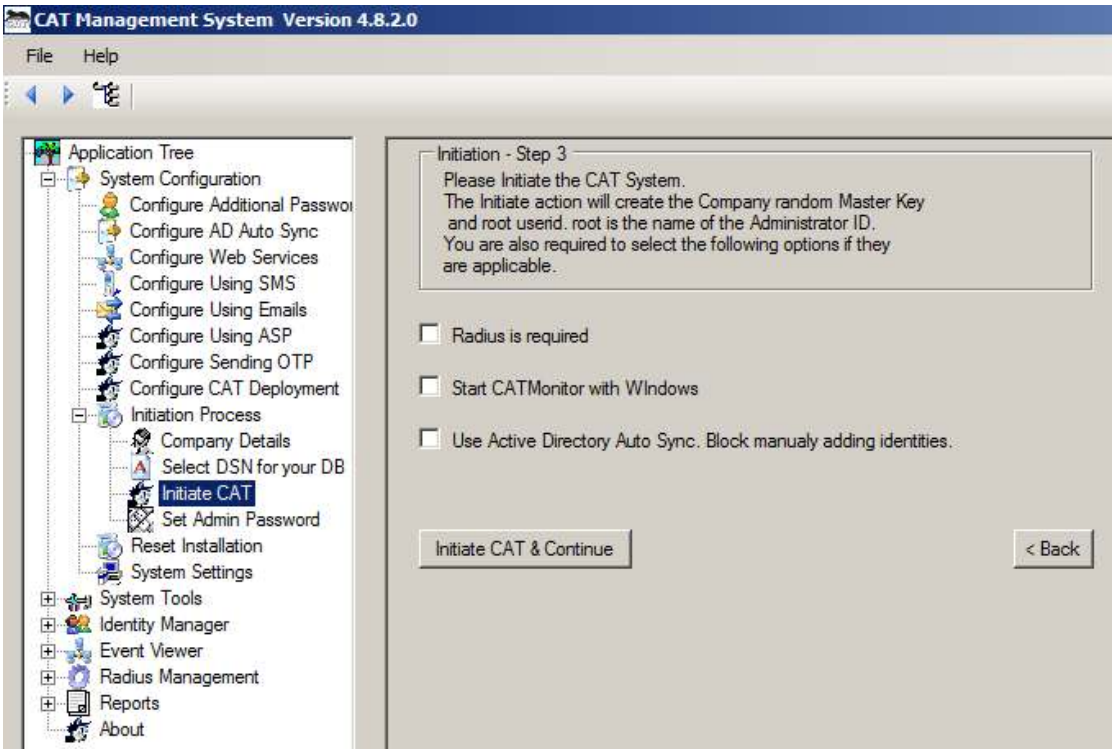
At this stage you can instruct the CAT MS to activate the Radius, CAT Monitor and choose to synchronize with your Domain Active Directory (AD).

The CAT Monitor is primarily needed for installations that are going to use the CAT Radius. The monitor:

- Shows the status of the Radius system service
- Allows the administrator to start/stop the service
- Has a shortcut to start CAT MS
- And more

For more details read The CAT provided Radius Server chapter.

Selecting the User AD Auto Sync will require a periodic synchronization with the AD. The Users' details will be taken directly from the AD and updated periodically as will be configured using the Configure AD Auto Sync option. When this option is selected, the CAT Management System is restricting the Administrator activities. The Administrator won't be able to define new users or update users' details as all the information is imported from the AD automatically.



Check the appropriate boxes and press the **Initiate CAT & Continue** button.

The CAT MS will take few seconds to check the database and:

- Create and store the installation master key
- Create and store the “root” user id. The “root” user id is the basic Administrator user id. It can only be used to access the CAT MS.
- Prepare the Radius setup files (if checked)
- Start the CAT monitor (if checked)

The Mega AS CAT Radius service does not start automatically after the installation. It will start automatically the next time your Server is started. Once the initiation has finished, you can start the service using the CAT Monitor.

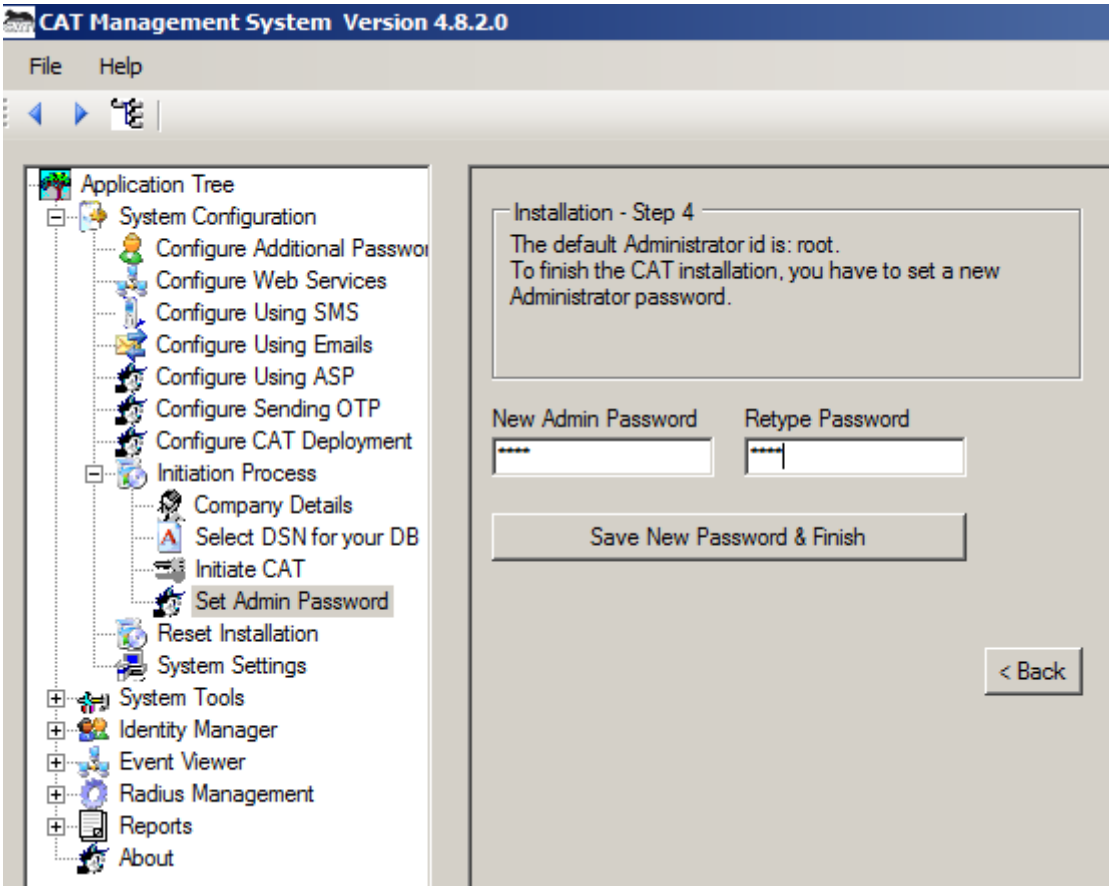
Notice: If you did not check the Radius is required option – you will not be able to use the CAT Radius Server. The Radius management options will not be included in the Application Tree.
If you do check the Radius option – you don’t need to use Radius. You can start using it at any stage later.

Initiation – Step 4

This is the last Initiation stage. Note – when upgrading to a new CAT AS version, this step is skipped.

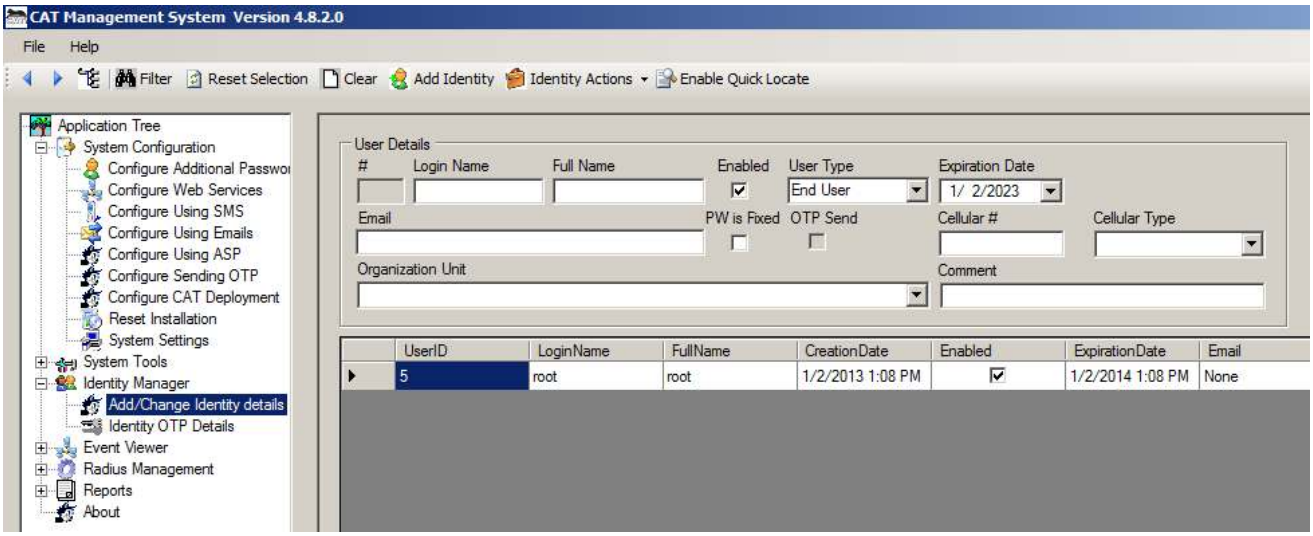
The system has already defined the “root” Administrator User ID.
The default password is blank. The system requires that you define a password for the “root” User Id.

We recommend at least 8 characters and numbers. Follow your organization Password policy to protect the system.



Press the Save New Password & Finish Button.

If the initiation was successful the system will open at the Users List window to allow starting adding new users to the system.



To learn how to add user, read the Identity Manager chapter.

The CAT Radius Server

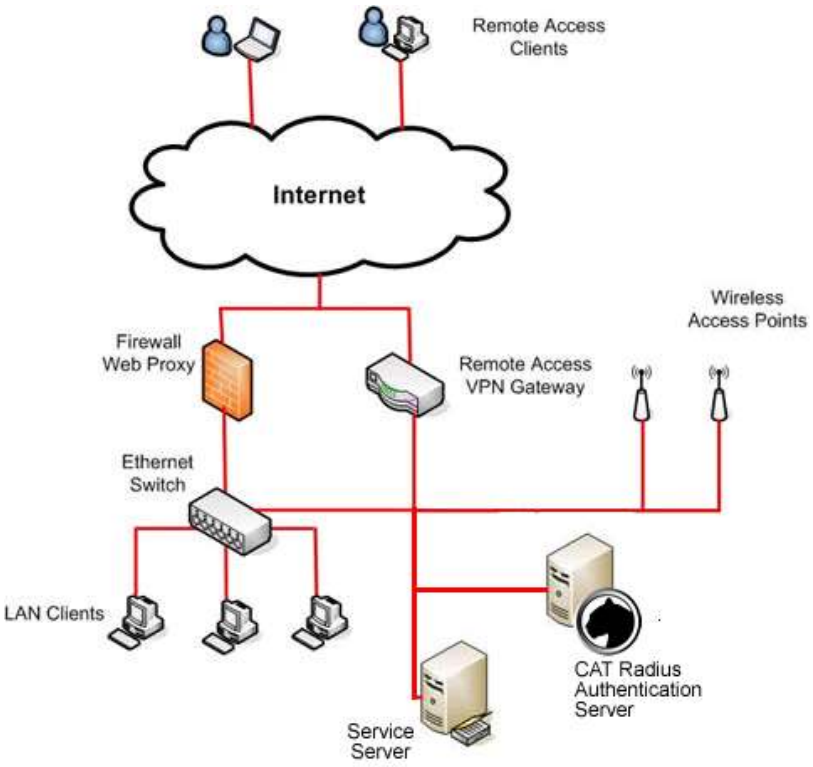
Radius – “Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service . Created by Livingston (now owned by Lucent)”, “RADIUS is a de facto industry standard used by a number of network product companies and is a proposed IETF standard”. (Olivier Thomas and Ciske van Oosten, 02 Aug 2006)

The Radius is a client/server protocol where a client (Network Access Servers) sends a request, which is responded by the server (RADIUS server).

The CAT provides is own Radius server to enable Radius clients Authentication queries to be handled by the CAT Authentication Server. The current version of the CAT Radius supports only PAP protocol.

For the Radius integration the System Administrator of the organization has to perform the following tasks:

- Define at the Radius client (VP, Firewall, Network etc) that the Authentication queries are delegated to the CAT Authentication Server. For this setup the administrator needs to know the IP address of the Server where the CAT MS was installed.
- Add the above client, to the Clients list of the CAT Radius. For this setup the administrator needs to know the IP address of the client generating the Authentication queries.



Initiation of the CAT Radius Server

When you check the “Radius is required” option in Initiation – Step 3 the CAT MS opens the menu options that manage the CAT Radius Server.

The CAT Radius is a Windows Service. Each time the Server boots, the CAT Radius Service starts. To monitor the service, you have to use the CAT Monitor.

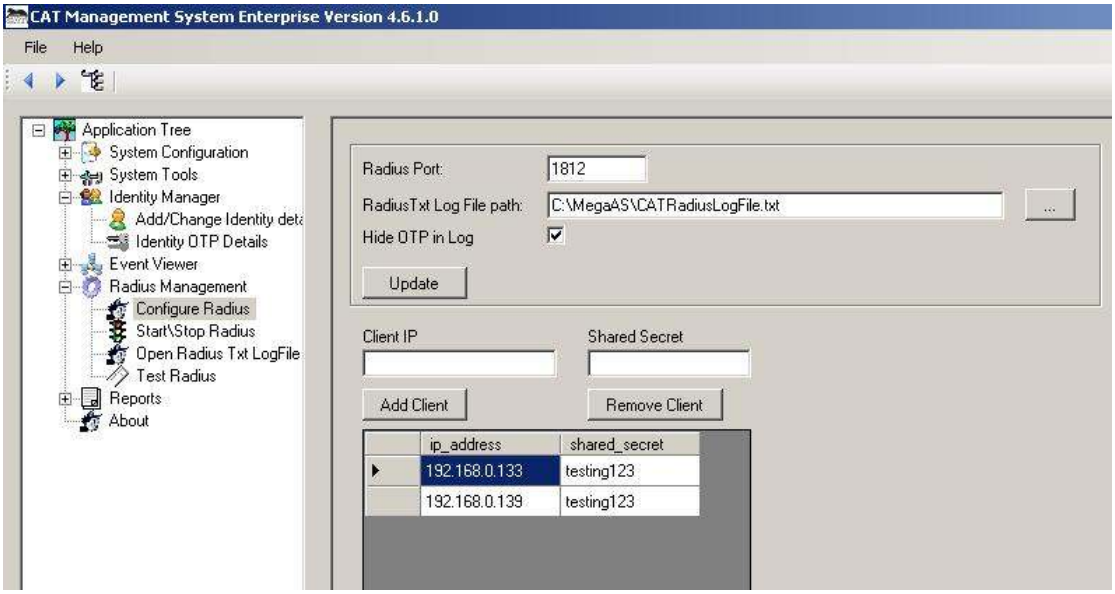
The CAT Monitor can be started from the CAT MS, but it is recommended that you check the option to start it automatically with Windows on your server.

If you did not check the Radius is required option – you will not be able to use the CAT Radius Server. The Radius management options will not be included in the Application Tree.

Configuring the CAT Radius Server

The Radius Server process is active all the time. The process is “listening” on the Server port and waits for incoming Authentication requests from Radius clients.

Radius Server has to “hear” the request – listen on the same port where the request is sent to, and the Radius Server has to know the client. Clients that are unknown are not answered and thus – denied access. The Client and Server also share a secret (password). This shared secret is used by Radius to encrypt/decrypt the Passwords entered by the end user. This way, the password is always secured.



The default Radius Authentication port is 1812. Some Radius clients may be using a different port. To change the port, enter the port number and press the Update button.

A Radius client is identified by its IP address. The Radius client message is interpreted by the common secret. The secret is used to encrypt/decrypt the Radius message. The same secret has to be defined at the Radius client and the Radius Server.

Notice – The CAT Radius requires that no other program uses the same port.

To add a new Radius client to the list enter the IP and Shared Secret data in the fields and press the **Add Client** button.

To remove a client, select the client using the mouse. The client data will appear in the data entry fields. Now press the **Remove Client** button.

If you entered or selected a text file for the **Radius Log** output, the service will try to log its messages in the file.

When the **Hide OTP in Log file** option is checked, all the passwords are replaced in the log with ******. If it is not checked, whoever opens the Log, will be able to see what password or OTP was used by the end user for Radius authentication.

Using the CAT Monitor

When the CAT Monitor is active, its icon appears at the Notifications area.
On the CAT Monitor Icon there is a red line when the Radius Server is down and green when the Radius Server is active. The icon does not refresh automatically. To refresh the icon, you need to right click on the Icon.

Right Click with the mouse button on the CAT Monitor Icon to get the Actions list.
Using the CAT Monitor you can control the CAT Radius service and the CAT AD Sync service if it was selected during the installation.

Notice - If the Radius data changed – the Radius port number or the clients list etc., to take effect, the Radius has to be stopped and started again.

The Monitor shows the status of the CAT services by a message and color.
It will color red the message if the service is not running and green if it is running.

If the CAT is not installed with AD Sync, the related options will not be available in the monitor menu.

Start CAT Radius in Normal Mode – the CAT Radius service will be restarted.

Start CAT Radius in Debug Mode – the CAT Radius service is stopped and the CAT Radius program is started in a debug mode. A console window will open and all the system messages will be printed in the console. The messages will also be written to the text Log File if you have entered a file path.

Stop CAT Radius – will stop the current running CAT Radius.

Manage Radius Clients – opens a quick window for adding or removing clients. For the changes to take affect the CAT Radius has to be restarted.

Set Radius Port - opens a quick window for changing the port number. For the change to take affect the CAT Radius has to be restarted.

Set Radius Log File Path Clients – opens a quick window for entering or changing the Log File path. For the change to take affect the CAT Radius has to be restarted.

Open Radius Log File – opens the text file as entered in the Log File path.

The following option will be visible if the AD Sync was enabled during the installation in Initiation – Step 3. The AD Sync had to be configured using the CAT Identity Management system.

Run CAT AD Sync now – if the AD Sync is enabled, this option will start the service and cause a soon as possible run of the AD Sync.

Stop AD Sync – will stop the service.

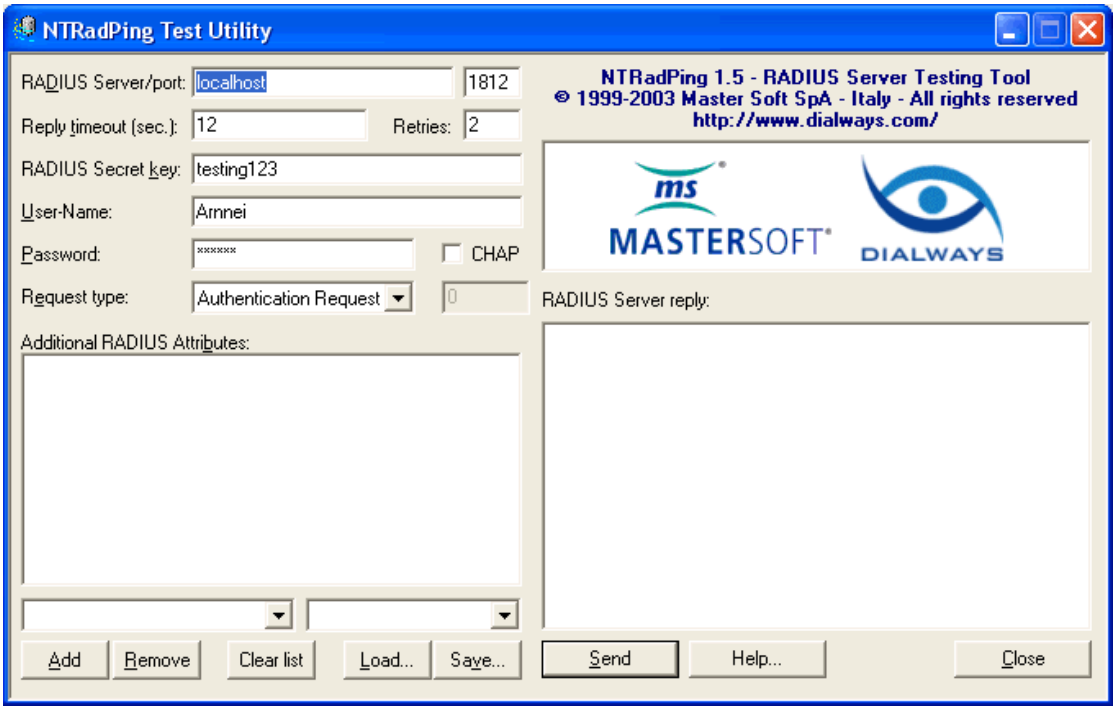
Open AD Sync Log File – opens the AD Sync Log File as defined in the CAT Identity Management system.

Testing the CAT Radius Service

To test the CAT Radius Server you need to run a Radius client that will generate an Authentication query.

Select the Test Radius option at the Application Tree. Read the instructions message and press OK to continue.

The CAT MS test option will open for you the NTRadPing – Radius Server Testing Tool (© 1999-2003 Master Soft SpA – Italy – All Right Reserved)



Check the CAT Monitor to verify that the CAT is running. The CAT Monitor icon should have the green line.

The NTRadPing is running on the local host – same PC as the CAT Radius Server.

Fill the required NTRadPing fields:

Radius Server: localhost (make sure that you have an entry for the local host as a client of CAT Radius Server. Have a look at the Configure Radius option)

Radius Port: 1812 (unless otherwise specified at the Configure Radius option)

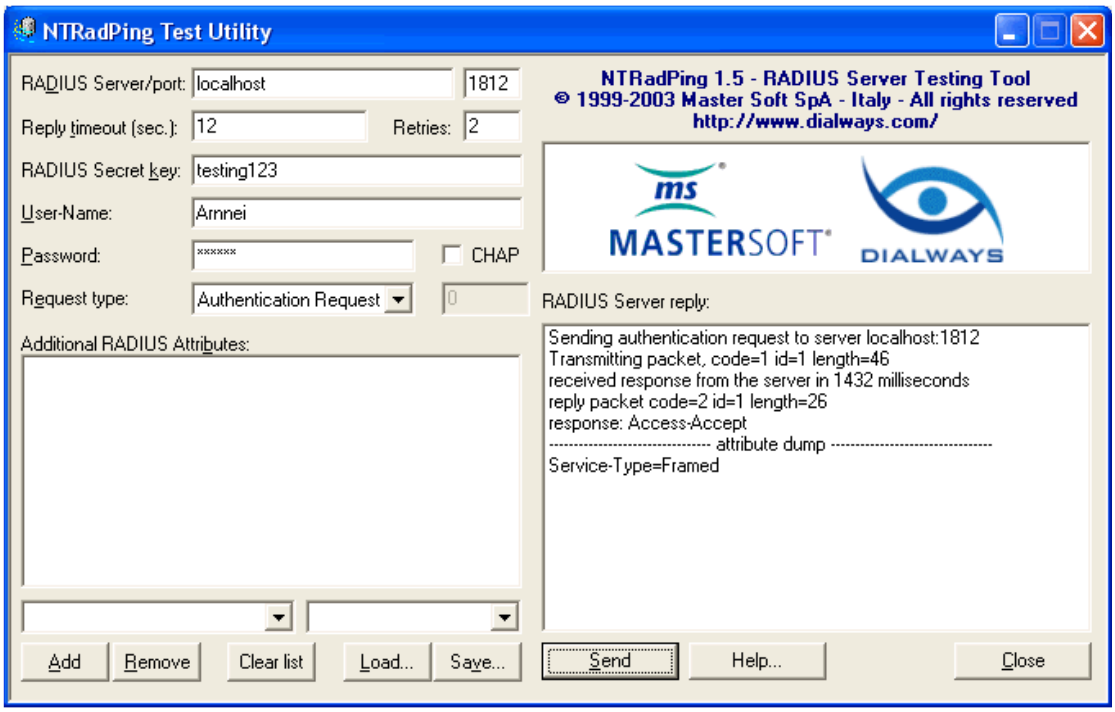
Radius Secret Key: testing123 (unless otherwise specified at the Configure Radius option)

User Name: (You cannot use “root”. You need to have at least one Identity defined. Have a look at the Add/Change Identity, Application Tree option)

Password: (That has to be the Identity/User One Time Password. To get the Identity OTP look at the Identity OTP Details, Application Tree option)

Request Type: Authentication Request

Press the Send button to submit the client Radius Authentication Request.



The CAT Radius Server reply is visible and can be analyzed.

To further analyze the CAT Radius Server response, you can run the CAT Radius Server in a Debug mode. (Check Start/Stop Radius, Application Tree option). When running in a Debug mode you can see the logic the CAT Radius Server is applying to its decision-making and why it has accepted or denied a specific Authentication Request.

Installing the CAT API Web Service (Optional)

The CAT AS API Service contains a set of methods that can be used for local and remote Web application.

Make sure that IIS is installed and started.

IIS Requirements:

- Framework 3.5 + 4.0 installed
- ASP 2.0 enabled
- For 64 Bit Servers, Ensure that the “Enable 32-bit Applications” attribute is enabled for the application pool: IIS >> Application pool >> DefaultAppPool >> Advanced Settings >> (General) Enable 32-bit Applications

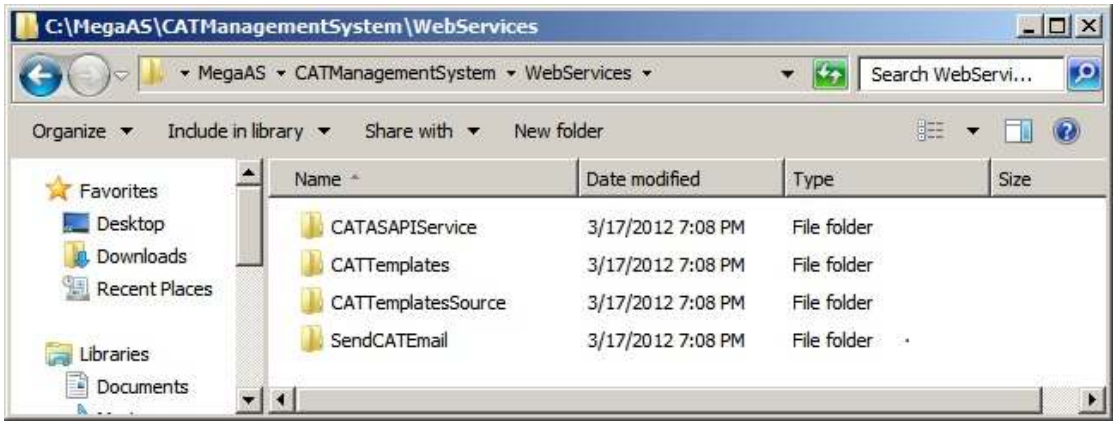
With CAT API Web Service you can:

- Use Active Pages to authenticate and register users. For example Login and Register Web forms.
- Send an OTP to a user Cellular Number via SMS or send an Email to his email address
- Easily deploy user accounts. The user does not have to add his CAT Token account manually (on some cellular OS only).
- Perform administrative actions. These actions are intended for Help Desk tasks.

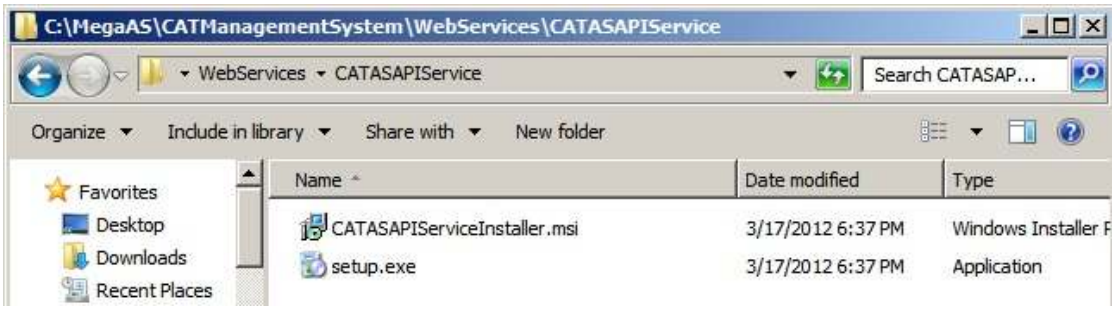
The CAT Templates is a full ASP.NET example of using the CAT API Service.

For an extended explanation read Chapter 4 – CAT Web Services

Find the CAT AS API Service at the c:\MegaAS\CATManagementSystem\WebServices folder.



Run the setup.exe to install the service.



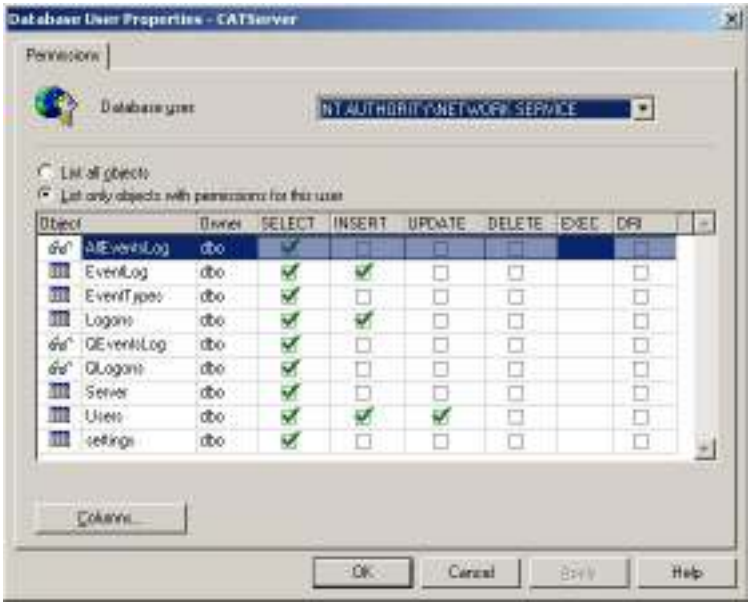
Next, open the CATTemplates folder and run the CATTemplatesInstaller.msi to install the API Templates sample site.

Next, define a DSN named: **CATAPIServices** the DB holding the Settings table. By default – it should be the same DB as your CATDB. You can use the Define DSN to Database option.

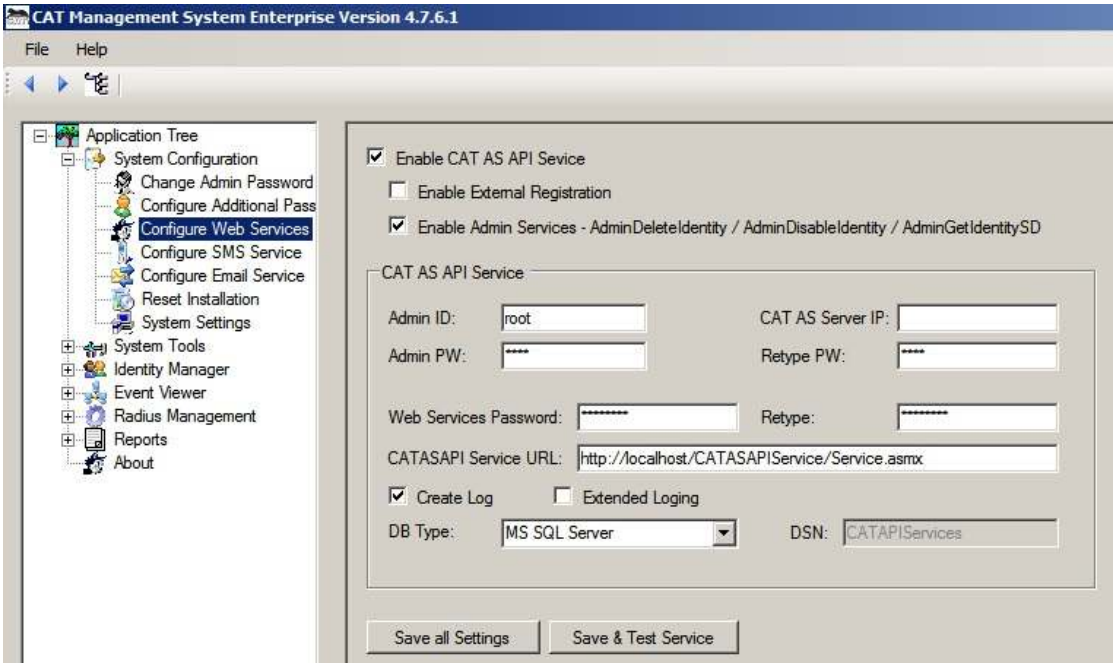
Notice. If you intend to enable the API Service to be used from Active Pages, the Database you are using should allow access to Network Services.

If you are using MS SQL Server you need to define the NT AUTHORITY\NETWORK SERVICE login in the Security folder.

Then, you have to make sure this user has the following permissions:



Enable the CAT API Service and save the settings using the Customize Web Services option.



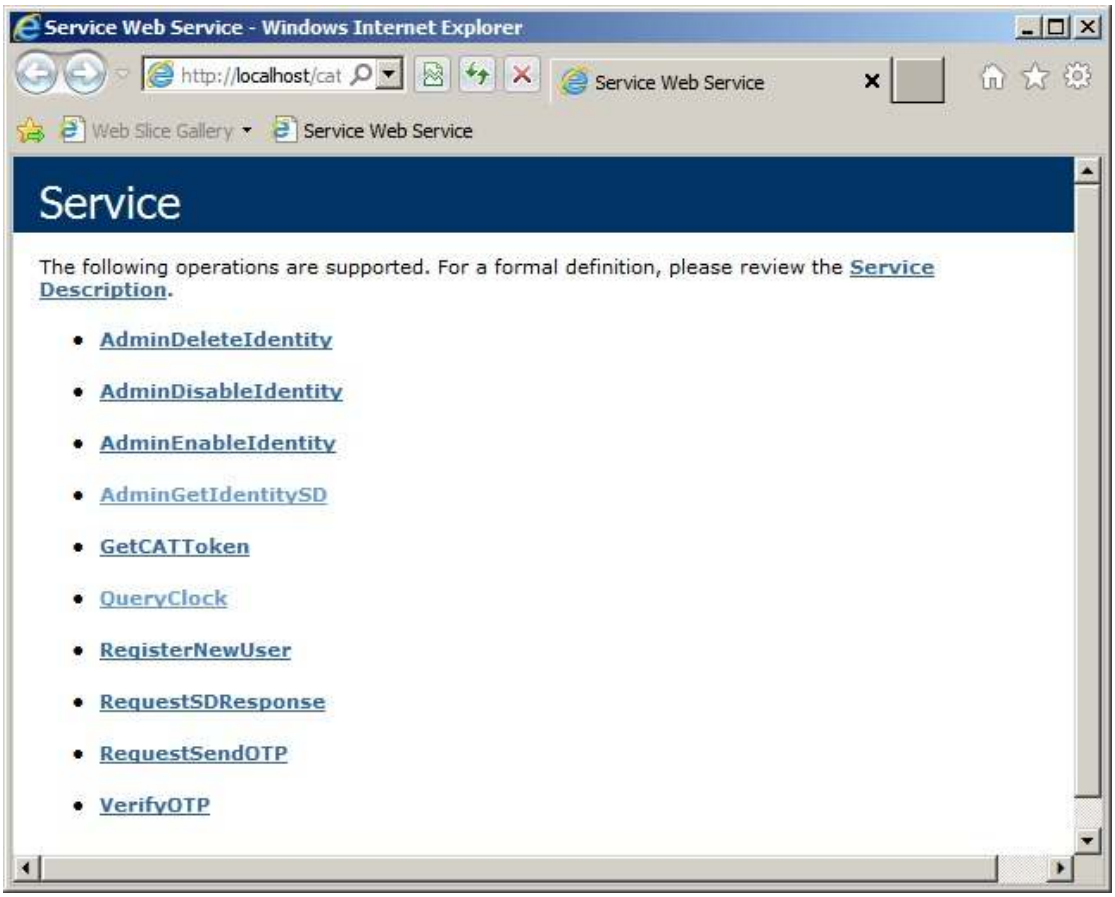
You may need to add NETWORK SERVICE permission to the CATServerDLL2.DLL file.

For an extended explanation read Chapter 4 – CAT Web Services

Testing the CATASAPIService

Open your MS Explorer and key in the local service address:
http://localhost/CATASAPIService/Service.asmx

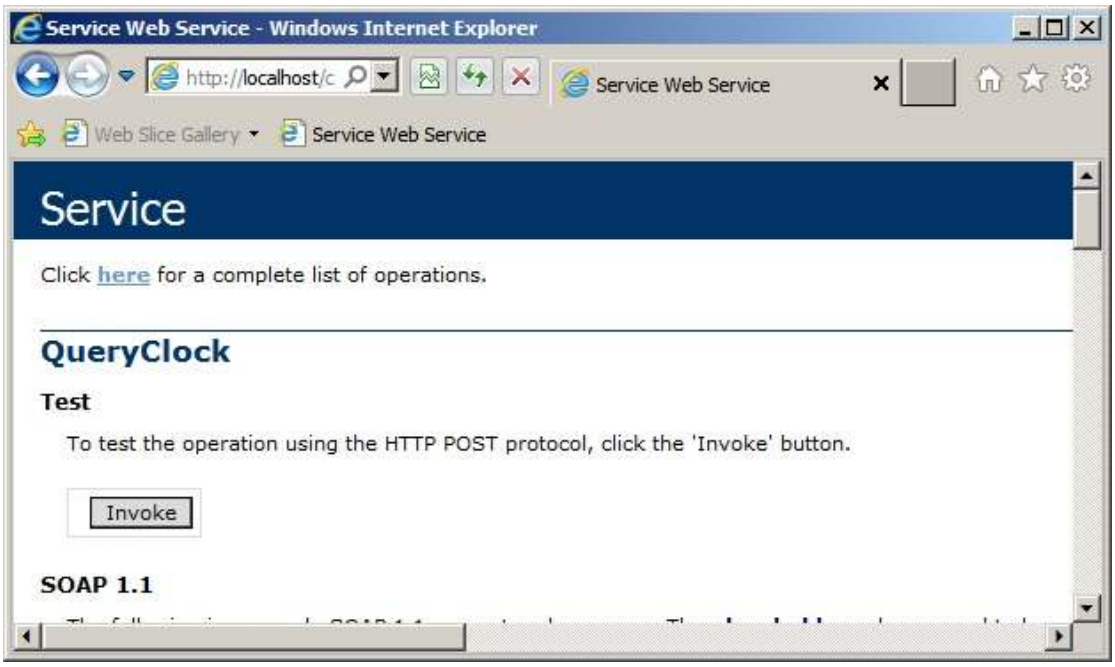
You should be getting:



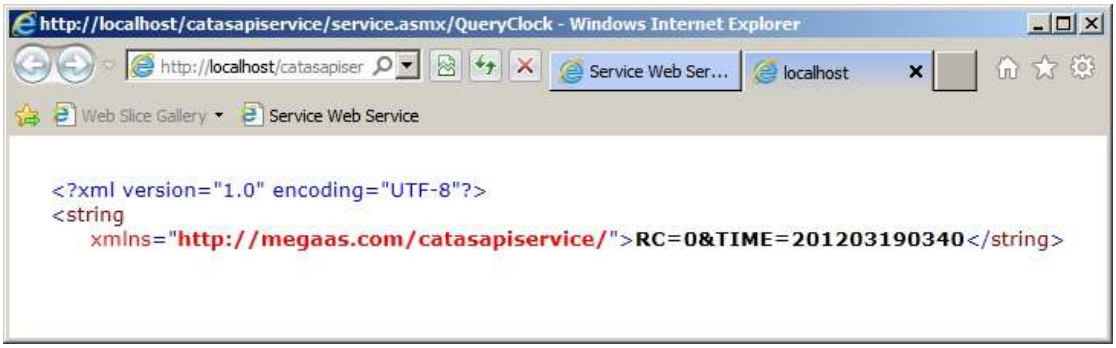
If you are getting Explorer messages, read the messages and correct your web site settings.

Errors at this stage are usually related to IIS enabling 32 Bit Applications or MS Framework 3.5 not fully installed. Also check that ASP.NET 2 is “Allowed” at the ISAPI lists.

Next, select the QueryClock method. You should get the Invoke form:



Press the Invoke button. At this stage you should be getting the method response which includes a return code (0 if all is ok) and the message which is a long date / time string.



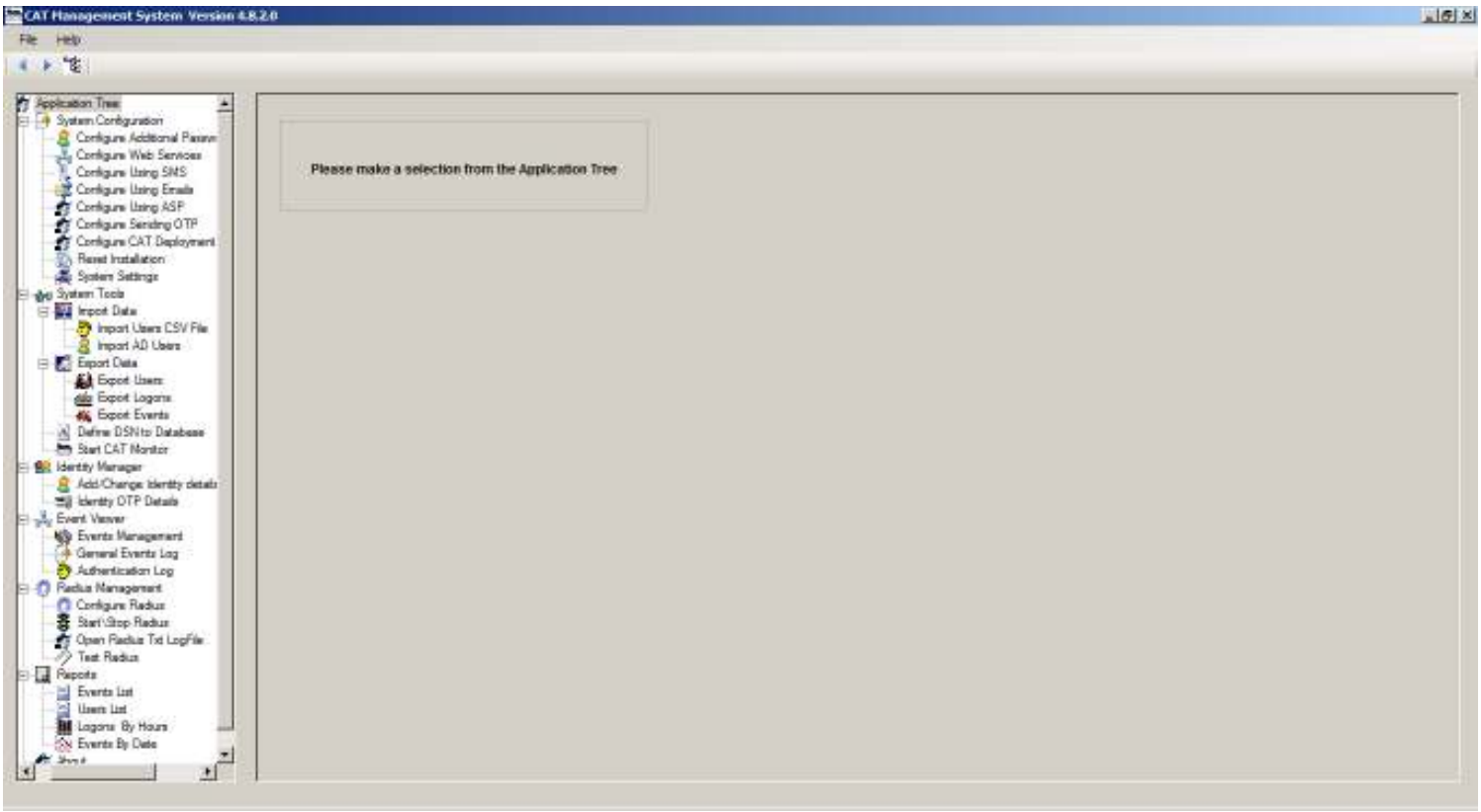
Errors at this stage are usually related to the Database authority of the anonymous user created by the IIS settings. The user can be in the form of: IIS_xxxxx or Network Services or another. This user should be allowed to access the CAT Server database and update the tables.

No errors at this stage mean that the service installation was completed successfully.

Chapter 3 – CAT MS Application Tree tasks

In this chanter we will go in details through each of the CAT MS Application Tree tasks.

The CAT MS Main Windows



The CAT MS main window has three main parts:

- Tool bars – the tool bars list options and icons change depending on the Application Tree selected task.
- Application Tree – the different CAT MS tasks.
- The Task form area – A task may be associated with a form. When selected, the task form will be in the Task form area. Some tasks open another window.

System Configuration

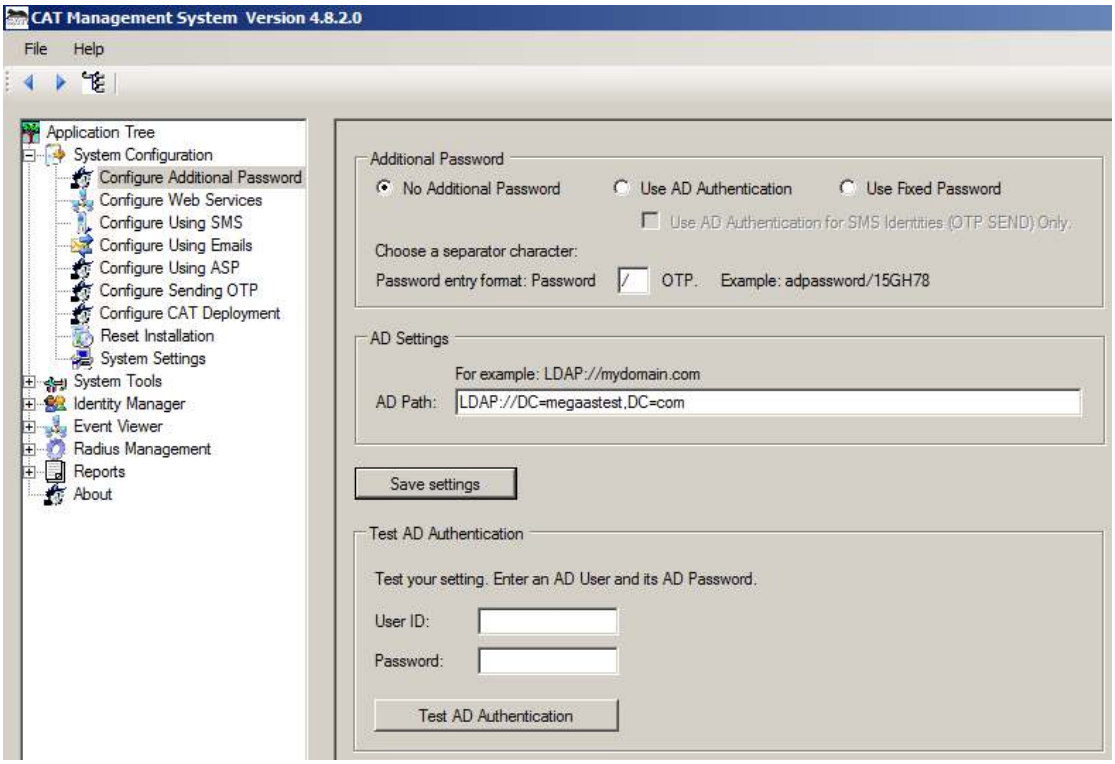
Configure Additional Password

Some installations may require in addition to the OTP authentication a fixed password for enhanced security. CAT MS can use the Active Directory user password or manage a user Fixed Password.

Normally (Default) the end user is required to enter his User ID and OTP for authentication. For enhanced security the administrator can select Use AD Authentication or Use Fixed Password. In this case, the end user enters into the Password field the Active Directory or Fixed password, a separator character and the OTP.

For example, if the end user's AD password is: 123456 and his OTP is: A67B89 and the separator is: /
The end user will enter into the password field: 123456/A67B89

CAT AS will split the string into fixed PW = 123456 and OTP=A67B89 and perform the AD or fixed password Authentication first, then if successful, CAT will check the OTP and return the result.



AD Path - enter the LDAP Domain Path string. The CAT will try to locate your default domain path. You can change it.

Separator character – the character that will separate between the AD password and OTP.

User ID – the test user id.

Password – the AD Password for the user id.

Make sure to test your AD settings when using the AD Authentication.

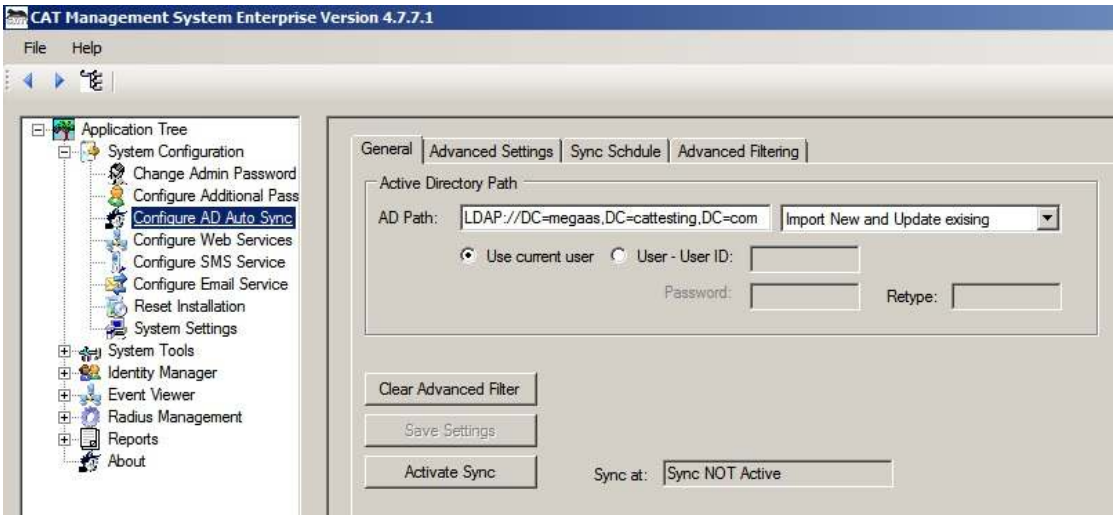
Configure AD Auto Sync

Active Directory is an implementation of LDAP directory services by Microsoft for use in Windows environments. Active Directory allows administrators to assign enterprise-wide policies, deploy programs to many computers, and apply critical updates to an entire organization. An Active Directory stores information and settings relating to an organization in a central, organized, accessible database. Active Directory networks can vary from a small installation with a few hundred objects, to a large installation with millions of objects. (Taken from Wikipedia - http://en.wikipedia.org/wiki/Active_Directory)

The CAT MS maintains its own functional database. Since the CAT MS DB is heavily used and has some internal special features it was decided not to use the Active Directory as the DB but to enable Identities Synchronization by importing Identities from Active Directory to CAT MS DB. The Automatic Synchronization allows the scheduling of a repeated Synchronization task.

CAT MS also provides a manual option for the occasional synchronization. (Refer to: Import Data (Import Active Directory Users))

The AD Auto Sync is enabled during the initiation. Enabling the Auto Sync means that **Identities MUST MATCH the Active Directory. The Administrator will not be able to manually add Identities and will have restricted ability to update Identities information using the CAT MS**. All updates has to be done in the AD.



General Tab

AD Path field – When you enter the Configure AD Auto Sync form the CAT MS will automatically identified the Domain that you are currently working in and will create the default AD Path string for you. The Path can be changed to refer to a remote server by adding the IP address. For example:

LDAP://192.168.133.199/DC=MyDomain,DC=com

You can also use other parameters to refine the import. For example if you want to import the users of an Organizational Unit called: Management at the local domain use:

LDAP://OU=Management, DC=MyDomain,DC=com

When you are making a partial import of existing users make sure you understand the behavior of the “Disable Missing Ids” option.

Once the AD Path has been defined you have to decide the AD Import type. You choose between:

- **New Identities.** Add to the CAT MS all the Identities that are in the AD but not in CAT MS. Remember that the maximum number of registered identities in CAT is dictated by the CAT Key that you have. The system will not allow importing more then that number. With this option you can not use the “Disable Missing Ids” option.
- **Existing Identities.** Update the existing Identities that are in the AD and in CAT MS. Since you are updating the already existing Identities, the system will not check the Can Import information field.
- **Both.** In this case, since you are also importing new identities, the system will check that you are not running over the Maximum registered users limit as defined by your CAT key.

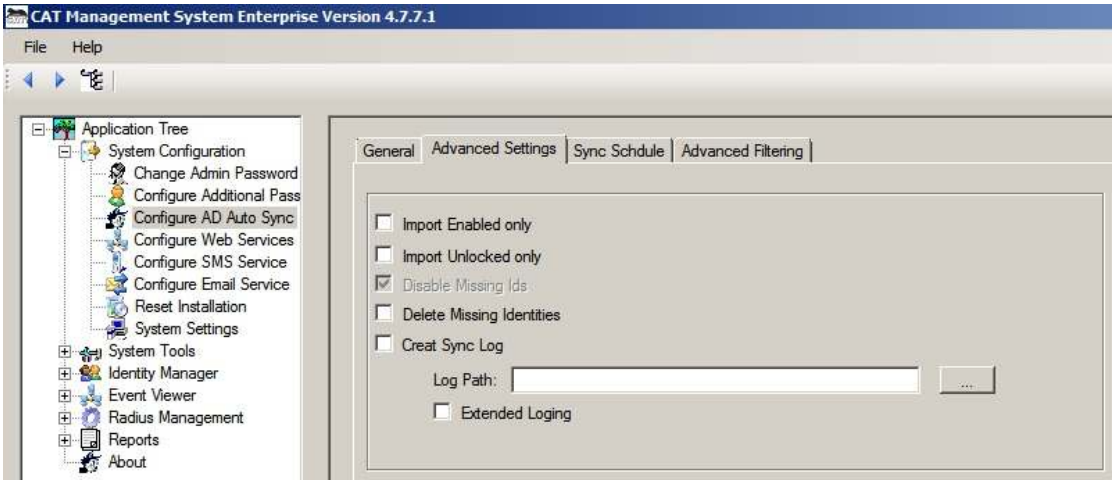
Use Current user or Use a different User ID/Password – Choose the credentials for accessing the Active Directory. Either use the credentials of current Windows user or enter another User ID/Password.

Clear Advanced Filter – clear the filter.

Save Settings (action button) – Once you have made your selections and entered the required values you can save the Sync details.

Activate/Cancel Sync – By default, the Sync is turned off. Once valid details have been stored, you can activate the sync. When you activate the sync, the system will calculate the expected next Sync time and follow the saved settings.

Advanced Settings Tab



Import Enabled Only - Only import identities that are enabled in the AD. Using this option in conjunction with the Disable Missing Ids is an efficient way to disable in CAT MS any Identities that were removed from the AD or were disabled in the AD.

Import Unlocked Only - Similar to the above, but only imports AD Identities that are not locked for any reason in the AD.

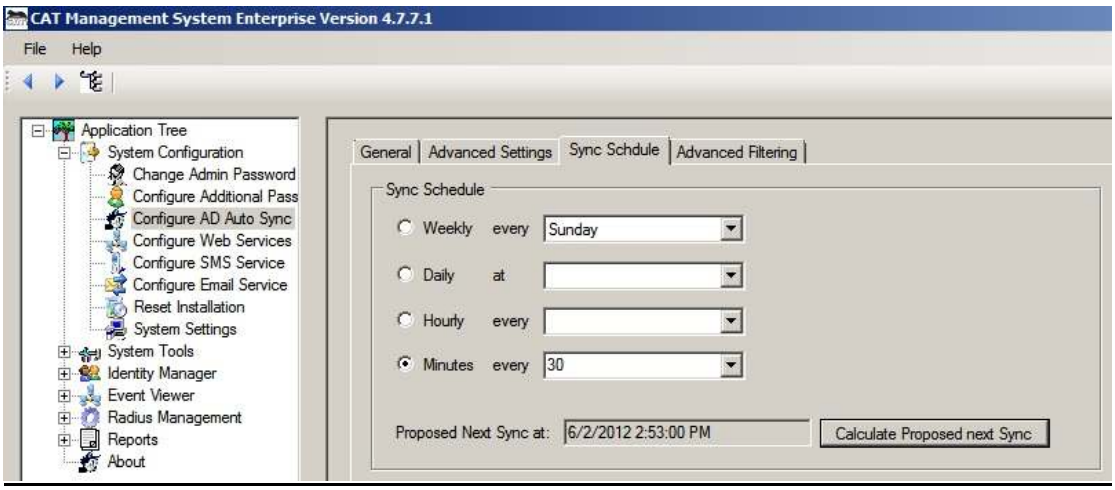
Disable Missing Ids option – This option is on as default. This option is running as a second step to the AD Import. Once all the existing users and new users have been updated in the CAT MS the system checks which Identities in the CAT MS WHERE NOT UPDATED. Those Identities are disabled.

Delete Missing Ids option – This option is an alternative to the Disable Missing Ids option. Once all the existing users and new users have been updated in the CAT MS the system checks which Identities in the CAT MS WHERE NOT UPDATED. Those Identities are removed from the CAT Management System.

Events Log – you can select to save the Sync log into a text file. You must provide a valid path. If the file does not exit, the system will create it.

Extended log – when selected, the generated execution log includes low-level messages that refer to the way the execution was carried.

Sync Schedule Tab



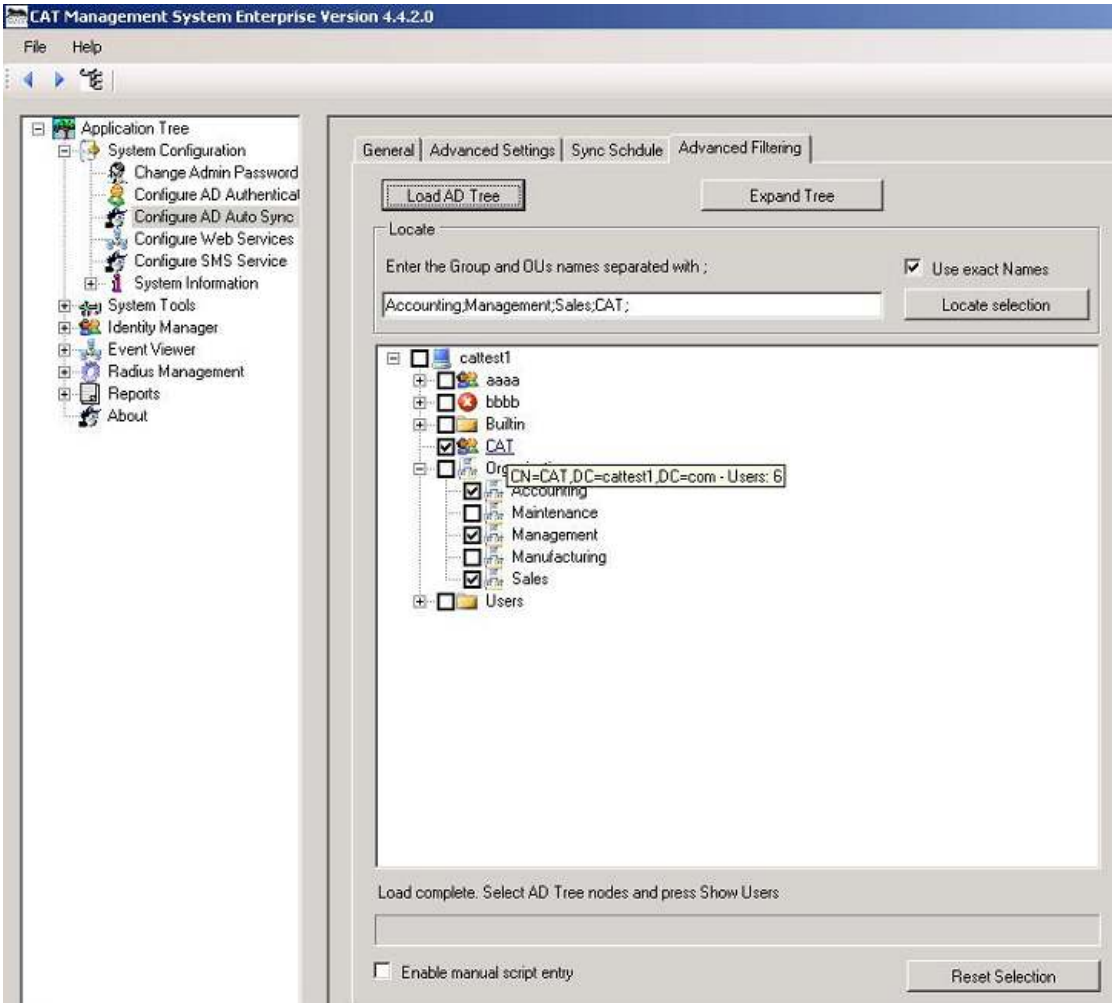
You can select between the following scheduling options:

- **Weekly.** Once a week on a given day of the week the system will perform the saved Sync.
- **Daily.** Once a day, every day at a given time the system will perform the saved Sync.
- **Hourly.** Every XX number of hours the system will perform the saved Sync.
- **Minutes.** Every ZZ number of minutes the system will perform the saved Sync.

Advanced Filtering Tab

The Advanced Filter builds the AD Organizational Units (OU) and Security Groups tree. Once the tree is built, any branch can be selected and the nested sub groups are selected as well. The selection is translated into a Filter script presented at the bottom of the window.

Press the **Load AD Tree** to display the domain AD tree. This action may take few seconds. Wait for the action to finish.



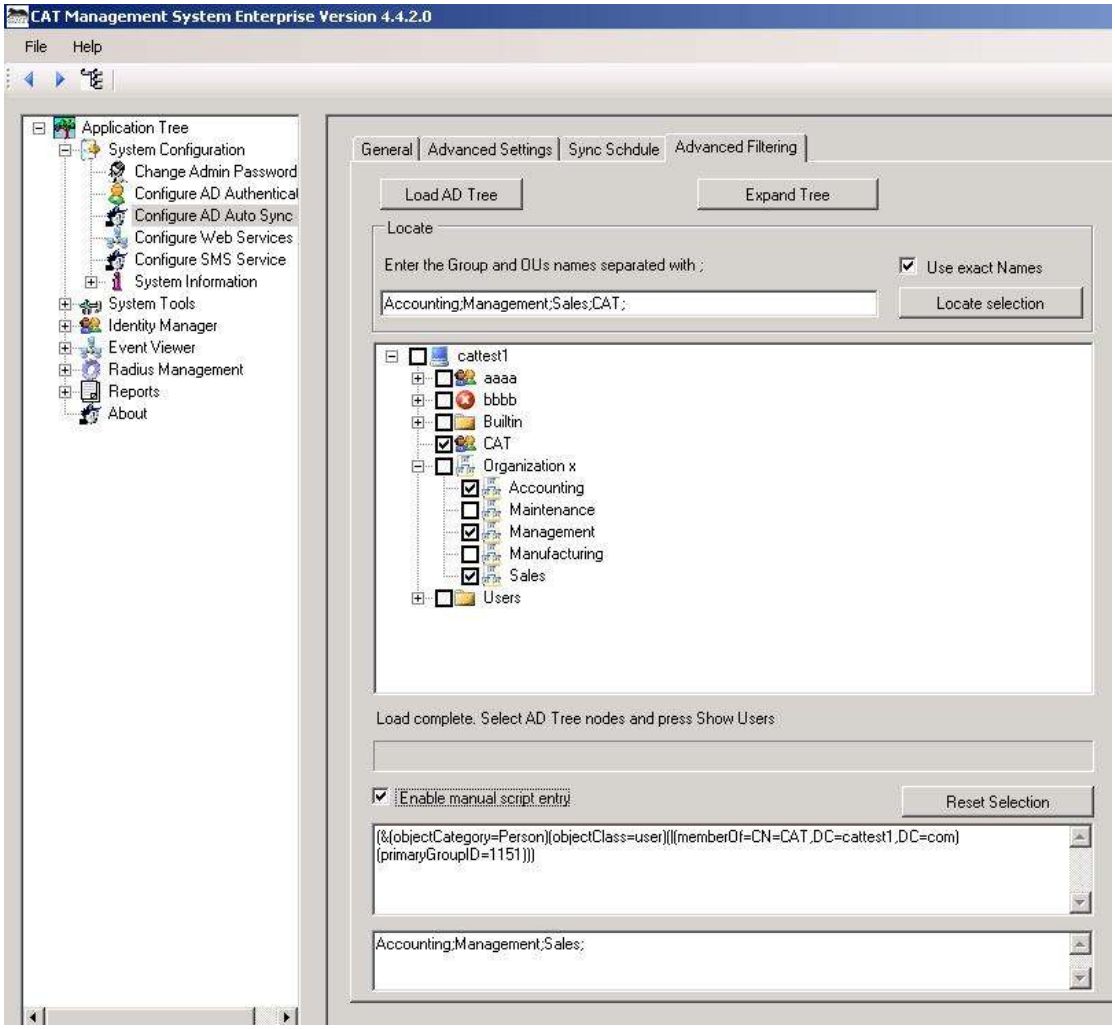
If no particular group or OU is selected then all the users are selected for the import.

The selection logic is OR between the groups, OR between the Organizational Units and AND between the two. For example, you selected the CAT security group and Accounting + Management + Sales OUs, the result selection will include all the CAT group members that are members of one of the selected OUs.

Notice – the selection of Groups AND Organization Units results in the intersection sub group as explained above.

To see the Filters script, check the **Enable manual script entry**

The administrator can modify the Filtering Scripts created by the system. We recommend that the entered script will be first tested at the manual option for the occasional synchronization. (Refer to: Import Data (Import Active Directory Users)) to ensure that the script works, and avoid Auto Sync failure.



The first text box contains the security groups AD Filter. The text is LDAP selection syntax. The text box bellow is the OUs selection. The text contains the names of the selected OUs separated by ;

The Expand tree button – spreads the full tree.

To search the tree for a specific group names or OUs just enter the names separated by ; and press the Locate Selection. To select exact names check the Use exact name, else the search will find all nodes containing the search names.

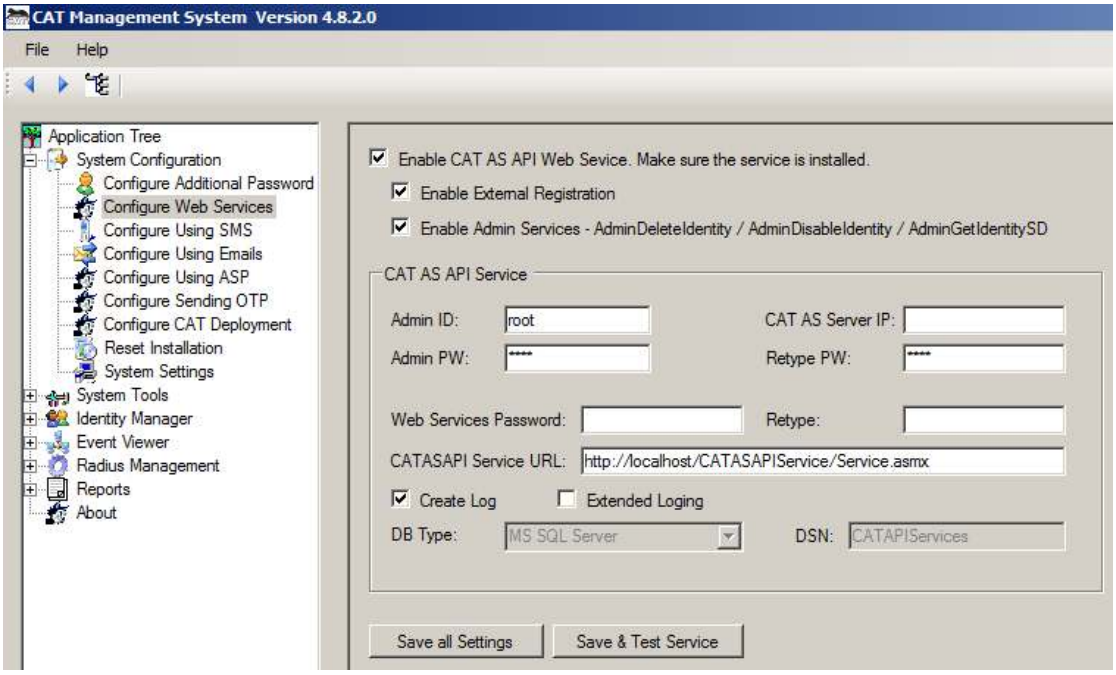
Check the example to the Locate Selection at **Advanced Filtering Tab** of the Import AD Users option.

Configure Web Services

The CAT API consists of a set of Web Services that enables you to easily call the CAT Authentication Server from other systems or build your own forms and windows to perform activities such as:

- Authenticate Identities
- Register new Identities
- Deploy SMS OTP or CAT Tokens to end users
- Query the CAT AS Time
- Manage Identities – Enable / Disable / Remove / Register and more

For an extended explanation and instructions using the Web Services read Chapter 4 – CAT Web Services



Enable CAT AS API Service – Check this option to enable access to the API Services from Active Pages. If the option is not selected you cannot save the settings.

Enable External Registration – Check this option to enable the specific API Service methods of registering new and update existing users to the CAT Authentication Server.

Enable Admin Services – Check this option to enable the Admin API Service methods of Removing / Enabling / Disabling identities and Viewing SD. These services are used to build a Help Desk Intranet service.

Admin ID – the default is the current logged in Administrator. We recommend that a specific user administrator will be added to CAT that will be used only for the Web Services. This ID is used when the API Service performs tasks that only an administrator is allowed, such as adding new identities.

Admin PW – is the Administrator Password

Web Services Password – Certain Web Services require a password to authenticate the calling web application. This password is for the developer to pass through the API for verification.

CATASAPI Service URL – This is the local CAT AS Server web service URL. It is used by the CAT for communicating with the CAT AS API Service.

Create log – If unchecked, the Web Service and CAT Management system will not log the Web Services activities at all

Extended Logging – Used for detailed log messages. Try the extended logging first and if the messages are too detailed, uncheck for reducing the amount of messages.

DB Type – is the same as the DB type selected for the CAT DB. The **DSN** named **CATAPIServices** should be pointing to the CAT database. By default this is the same DB as the CATDB.

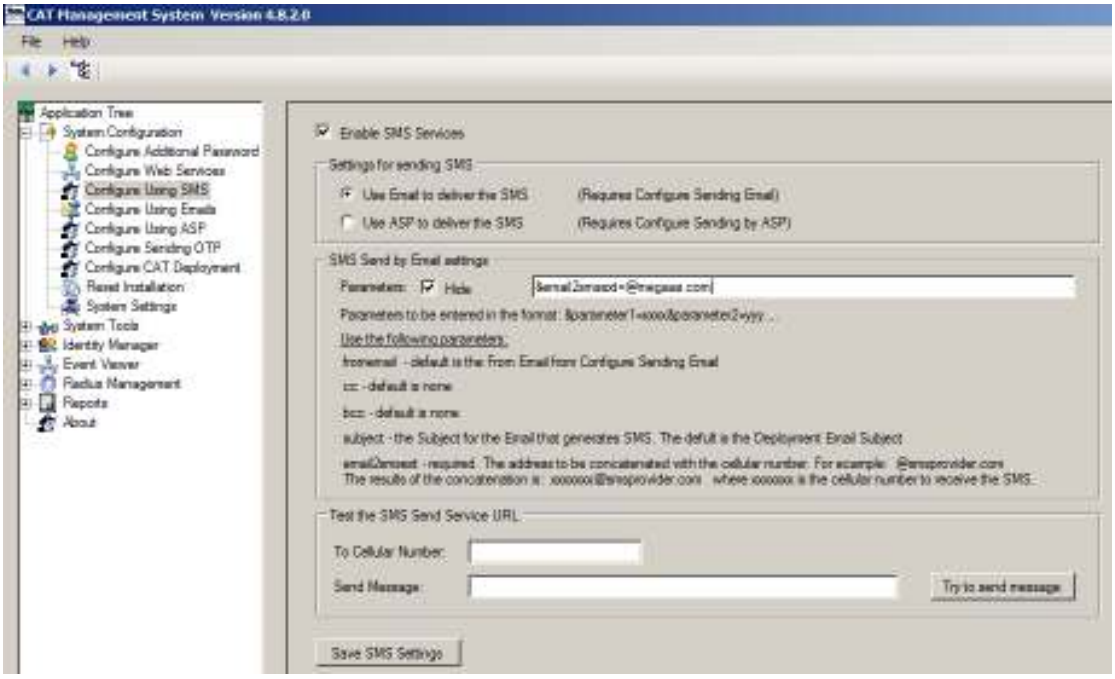
Press “Save Settings” to save the defined settings. The settings are saved as text file in the settings table legacy database at the enterprise web server.

Press “Save & Test settings” to save the settings and also perform certain tests on the services methods.

Configure Using SMS

SMS Services can be used to deliver certain messages such as OTP to an existing user, or to send CAT deployment URL to identities. To use SMS you need an SMS provider.

Using this option you can configure the connection with your SMS provider.



SMS Providers may have a number of APIs to receive and send the SMS to the target cellular number. The CAT supports two options that cover all.

Enable SMS Services – check to enable using SMS Services. When this option is selected, you can choose to deliver content using SMS for example OTP and Deployment URL.

Settings for Sending SMS – The CAT AS allows two methods of communicating with the SMS provider:

- **Use Email to Deliver the SMS** – Most SMS providers has an Email type API for sending SMS. Usually, the Email *Subject* of the email contains parameters for the API, the *To* address contains a concatenation of the identity Cellular number with the SMS provider domain and the Email *body* contains the SMS Message.

- **Use ASP to deliver the SMS** – All the relevant Identity information (cellular number, email, name…) and the SMS message are passed to an ASP page that will process and connect to the SMS provider using an API provided by the SMS provider. This option is an open customization. The ASP URL is provided in the Configure Using ASP option.

  When using this option, you build an ASP (Active Page) and configure whatever your SMS provider API requires. Upon request to send the SMS the CAT AS will create a URL string the will like for example:

  http://localhost/asps/sendsms.asp?email2smsext=@megaas.com&cellularno=44709781123&smsmessage=Your new OTP: 978345

  the http://localhost/asps/sendsms.asp url is defined by the administrator in the Configure Using ASP task.

  email2smsext parameter is defined by the administrator in the parameters field and passed to the ASP.

  cellularno parameter is passed to the ASP by the CAT AS. The cellular number is taken from the identity information. Other parameters containing identity information are also passed to the ASP. Those parameters are:

    email – containing the identity Email address

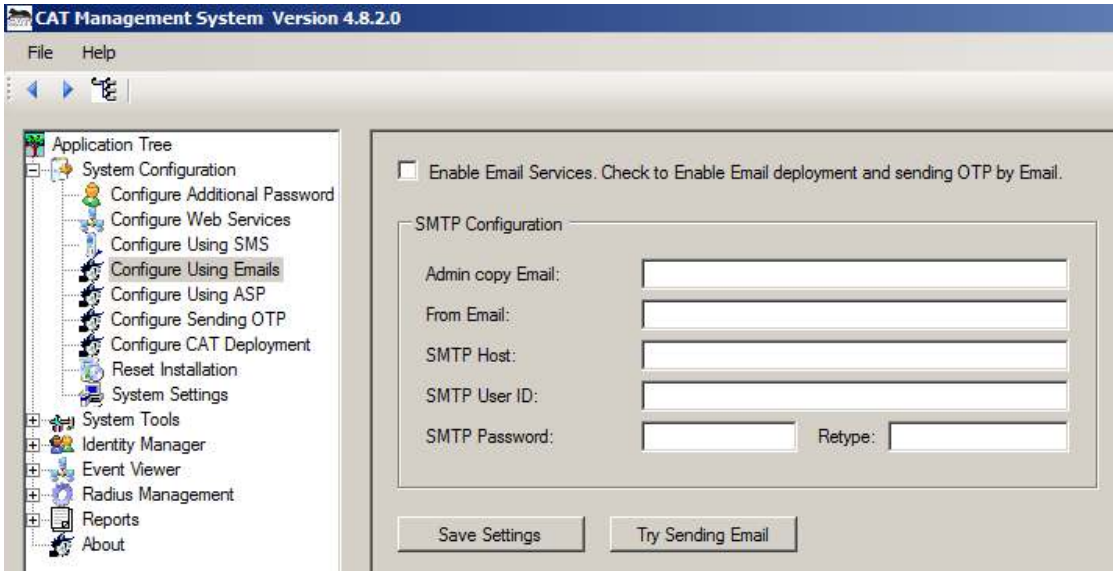
  smsmessage is passed to the ASP by the CAT AS. The message body is built by the CAT AS as defined in the Configure Sending OTP or Configure CAT Deployment.

Press “Save SMS Settings” to save the settings.

Configure Using Emails

Certain CAT AS messages can be sent using Emails. For example - deployment Emails to selected end users and/or OTPs.

The Email is sent through an SMTP server and details of the server have to be defined to the system using the SMTP Configuration fields.

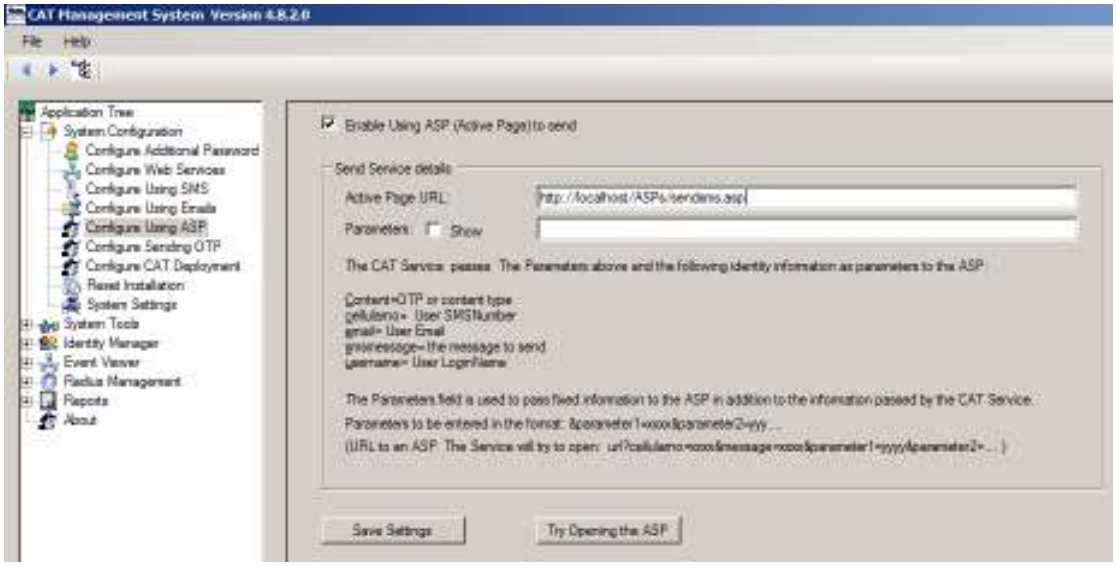


To be used, the Enable Emails Services must be selected.

The Try Sending Email will send an Email to the Admin copy Email.

Configure Using ASP

Active Page (ASP) can be used to configure an API to other systems for sending messages. The ASP is defined once and the same ASP serves – sending OTP by the Radius Server, sending deployment messages from the CAT MS to selected end users and the CAT Web Services.



The ASP is executed as a URL POST and a number of &parameters are passed to it:

- &cellularno=nnnnnn – the identity cellular number.
- &email=xxxxx – the identity Email
- &smsmessage=xxxx – the message body. The message body is built by the CAT AS as detailed in the appropriate Configuration task.

Some &parameters are added or specific services.
The Radius Server adds the following parameters:

- &content=xxxxx – The value is OTP for sending OTP.
- &userid=xxxxx – the end user Login Name
- &username=xxxx – the end user Full Name

Active Page URL – The ASP URL.

Parameters – Specific fixed parameters to be concatenated to the URL when posting. The parameters are to be defined in the format: &param1&parame2…. No comas or blanks.
The Parameters are entered securely and hidden by *, if you want to view the text – check the **Show** field.

When you build the ASP, remember to return "RC=0" when successful or "RC=nn&ERROR=errortext" when failed. The CAT will be looking for those return values.

Pressing the Try Open the ASP will POST the URL and pass the parameters. It will also show the result (return) values.

Configure Sending OTP

CAT AS supports sending OTP on request.

Check the **Enable the send OTP** Service for the following options to be available.

By default, all the identities are set to use OTP generated using CAT Token. For a specific identity to be set to use Sent OTP – you need to update that identity in the Add/Change Identity Details task (Check the OTP Send option for the identity and update).

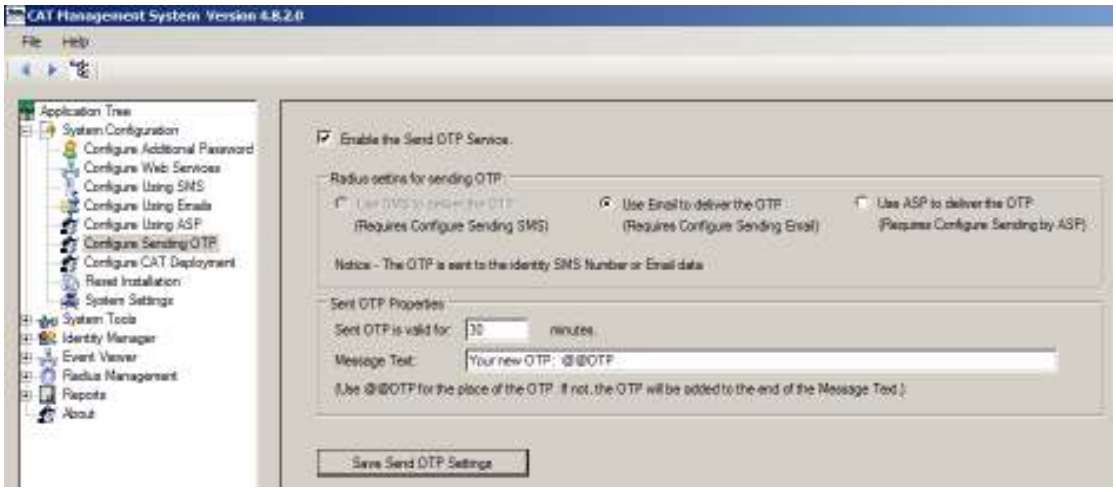
The request for OTP can be generated by:

- **Radius Server** – to generate a request for OTP by the Radius, you have first to Configure Additional Password to use Active Directory or Fixed Password in addition to the OTP. In the Radius Client, you need to configure a two stage Radius Authentication request. The first stage: the end user enters his User ID and his Active Directory or Fixed Password. The CAT Radius checks that the user is on OTP Send and that the AD/Fixed Password is correct. It will than try to send the OTP according to the settings bellow. The Radius client will get an Access Challenge response and will wait for the end user to type the OTP he/she received to make the final validation.

- **CAT Web Services** – using the RequestSendOTP function.

Radius settings for sending OTP – you can choose to send the OTP by one of three methods. To be able to select the requested method, you have to enable the method first and make the required method settings:

- **Use SMS for sending OTP** – Use the Configure Using SMS to enable this method.
- **Use Email to deliver the OTP** – Use the Configure Using Email to enable this method.
- **Use ASP to deliver the OTP** – Use the Configure Using ASP to enable this method.



Send OTP is valid for nn **minutes** – the OTP can be used once and will expire after 30 minutes by default. You can change the expiration time length.

Message Text – The OTP message is planned to be short. You can enter a default text for the message and use replaceable parameters such as the @@OTP.

Configure CAT Deployment

There are a number of CAT Tokens developed for cellular OSs and for Windows OS Desktop/Laptop.

The Deployment of the CAT Tokens is designed to be as easy and smooth as possible from the administrator and end user point of view.

Deployment can be done by the administrator from the Add/Change Identity Details task and using the CAT Web Services.

Deployment is the delivery of the CAT soft token, installation on the Cellular or Windows OS) and setting the Identity details in the CAT, to start viewing the identity OTP.

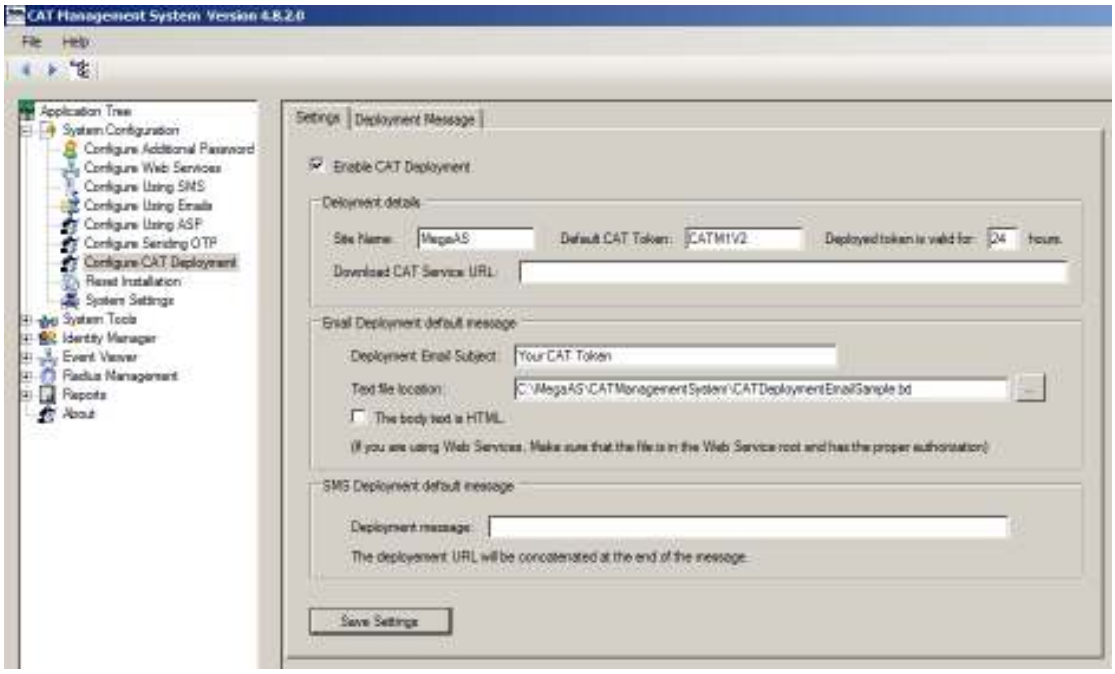
There are 2 parts in the deployment:

- Installing the CAT soft token – Installation is done like an installation of any other software on the device. Usually it will be done by downloading the software from the Internet using a link URL. This link can be keyed manually, or **sent to the cellular by SMS or Email**.

- Setting the Identity details – The setting requires 3 items (the rest are defaults). 2 of which are for information only and the third is the Secret Data (seed) that is calculated by the CAT. All 3 items has to be entered into the identity details on setup. The data entry can be done manually >> select the CAT menu >> select the Add Site Manually >> enter the data into the 3 fields and save. The other option (available on most of the CAT soft tokens) is to **send a Set-up String to the end user (by SMS or Email)** the end user uses Copy to copy the string and Past into a Paste field using the Add Site by Paste, CAT menu option.

Both the download URL link and the Set-up String can be sent in the same SMS or Email, using the Deployment options. For security, delete the message after setting the identity.

Since the Set-up string contains the Secret Data which is the basis for calculating the OTP, the administrator has an option to send the Set-up string with the Secret Data encrypted. In that case, when pasted, the CAT will request a password to open the Secret Data.
For more information read the Add/Change Identity Details chapter.



Setting Tab

Enable CAT Deployment – check to enable the service.

Deployment Details:

Site Name: The company or web site name. This is one of the required items for the CAT settings. It is used for information only.

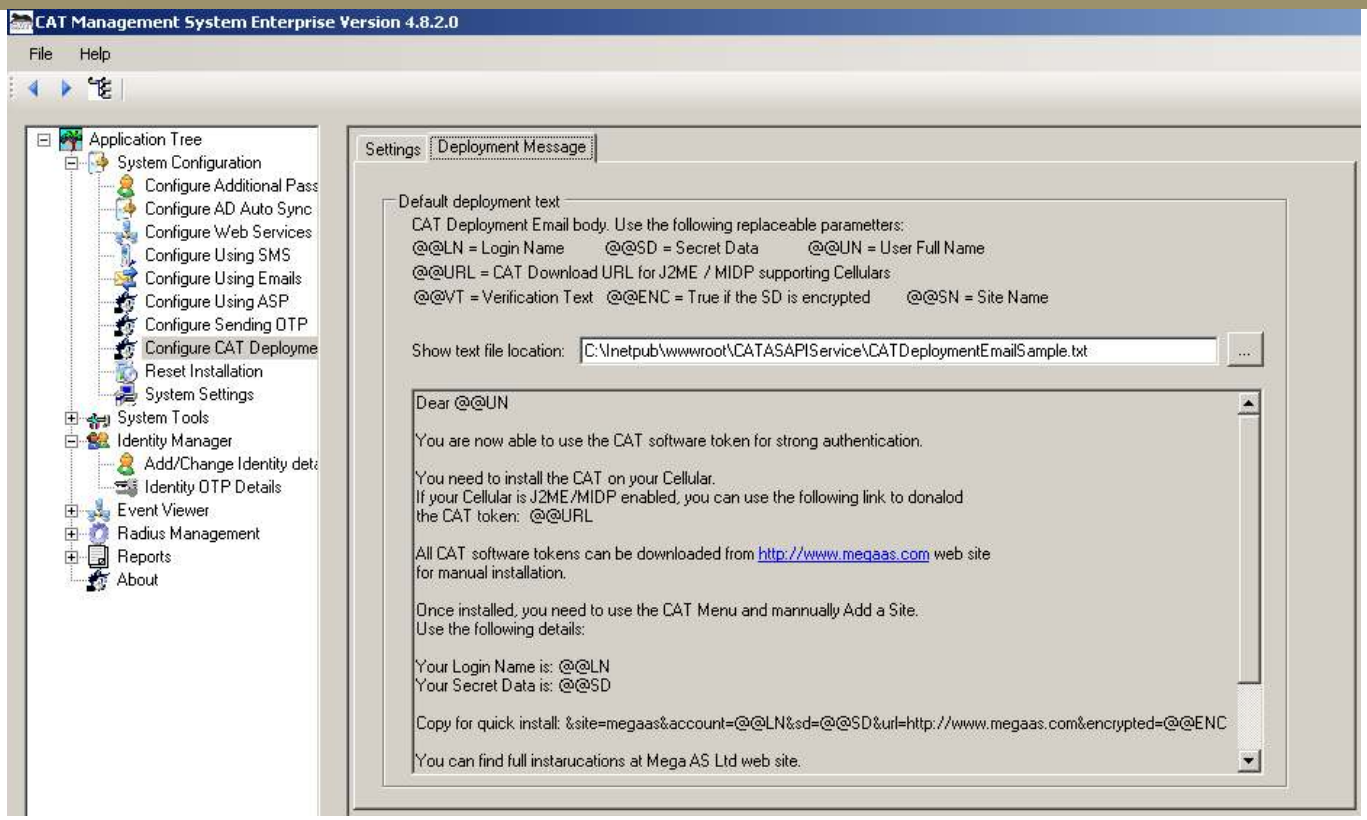
- **Default CAT Token**: This field is currently not used. Just enter CATS2.
- **Deployed Token is Valid for**: This field is currently not used. Leave the default.
- **Download CAT Service URL**: This field is currently not used.

Email Deployment:

Installing the CAT creates a sub folder called: CATDeploymentMessages. This folder contains a number text files each is a message template to be sent to the selected identities. You can also create any number of your own template files containing Email body for Email deployment.

A template can contain plain text or HTML script, with replaceable parameters. A replaceable parameter starts with @@ and a short string. When the deployment message is sent to a selected identity, the replaceable parameter is replaced by a value from the identity details. For example @@LN will be replaced with the selected identity Login Name.

You can see the full list of the support @@ replaceable parameters in the **Deployment Message tab**. This tab is used to display the selected message template file. Editing template messages is done by text editors outside the CAT MS.



In the example above the template that was selected contains a number of @@ replaceable parameters. This example is provided in the CATDeploymentMessages sub folder as you can see in the Show text file location field.

The supported replaceable parameters list is seen above the entry field.

The settings are the defaults. The Administrator can select another template file to send, during the Deployment task or choose to use the default.

Reset Installation

The Reset Installation task is an extreme method to reset the CAT AS.

The task will remove all data and registration keys and will revert to the pre initiation stage.

The next time you start the CAT MS, you'll be required to go through the initiation steps from the beginning.

Notice: All the users' data is removed and all Registry settings. **When the same users are recreated, they will have a different Secret Data.**

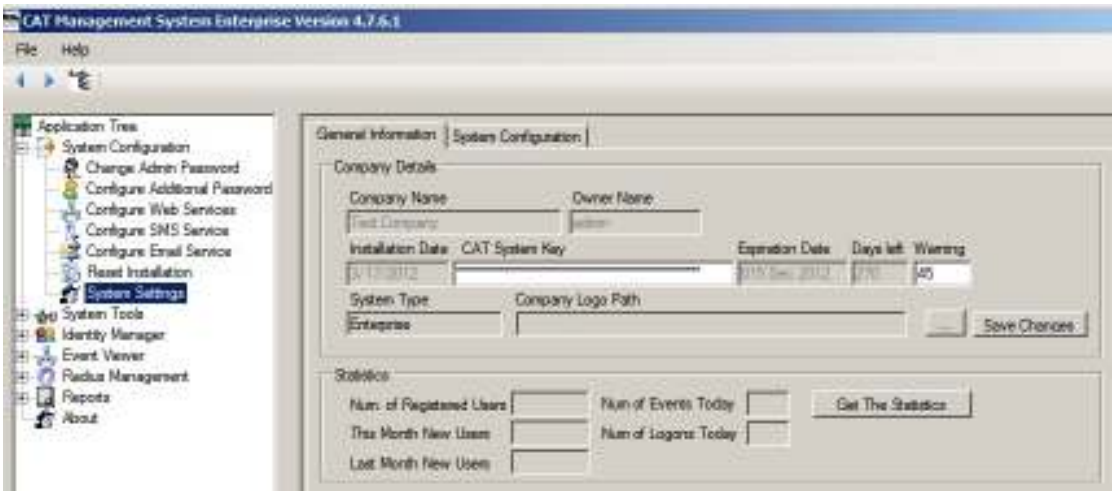
System Settings

The current setup form provides information about the installation and few fields that can be changed.

There are two Tabs:

- General
- Settings

General Information Tab



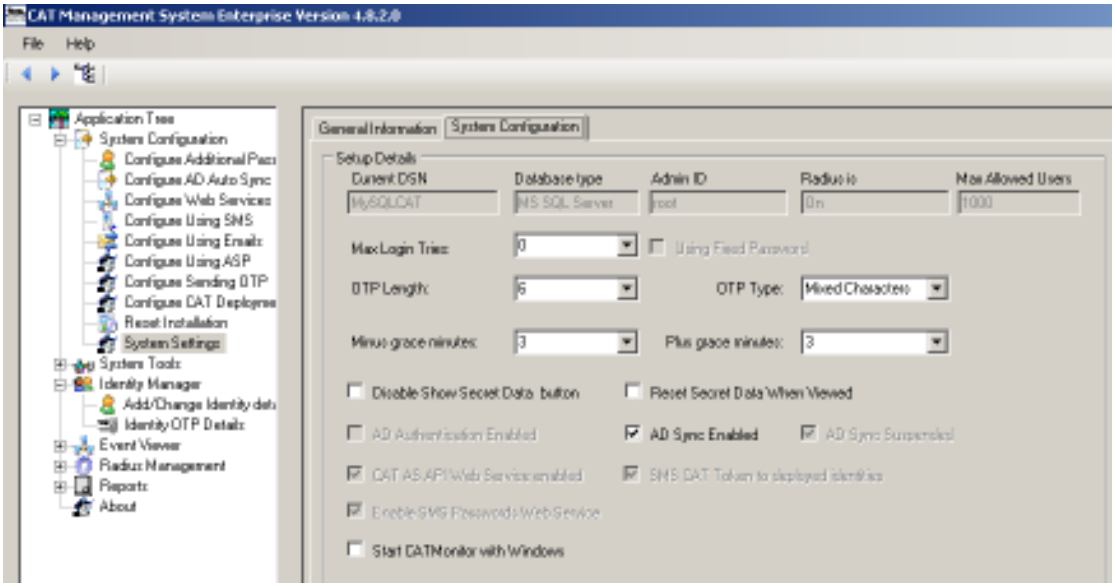
CAT System Key - The CAT Key is time limited. The Expiration date provides the expected expiry date of the Key. You can see the number of days left in the Days Left field.

When the CAT MS is used and the number of Days Left is less than the Warning number of days, the CAT MS will issue a warning message. When the number of Days Left is less than 0 the CAT MS will stop working.

Make sure to get your new CAT Key during your Warning Days.

When you have a new CAT Key you can enter/paste it into the CAT System Key field and press Save Changes to submit the new Key.

System Configuration Tab



The Max Login tries – after the defined number of failed Login tries, the user will be disabled. When the number is set to 0 (Zero), the Max Login tries is unlimited (it is not checked).

OTP Length – OTP length can be any even number between 6 to 12. Default is 6.

OTP Type - The Administrator can decide between two types of OTP:

- OTP that contains a mix of numbers and characters (default)
- OTP that contains only numbers.

Notice - the user has to match the OTP configuration in his CAT Token. On the Cellular, each Account/Site can be configured with the same options as above.

Time Grace Plus/Minus – the Administrator can define a time grace for cases when the user Cellular time is not matching the CAT Authentication Server time, but is close enough. The default is +/- 3.

Disable Show Secret Data button – Disables the Show Secret Data button in the Identity OTP Details form.

Reset Secret Data When Viewed – the default is to reset (change) the SD each time it is viewed or sent.

AD Sync Enabled – you can select to Sync the CAT managed Identities with the enterprise Active Directory repository. Enabling the AD Sync adds the Configure AD Auto Sync task to the tasks tree.

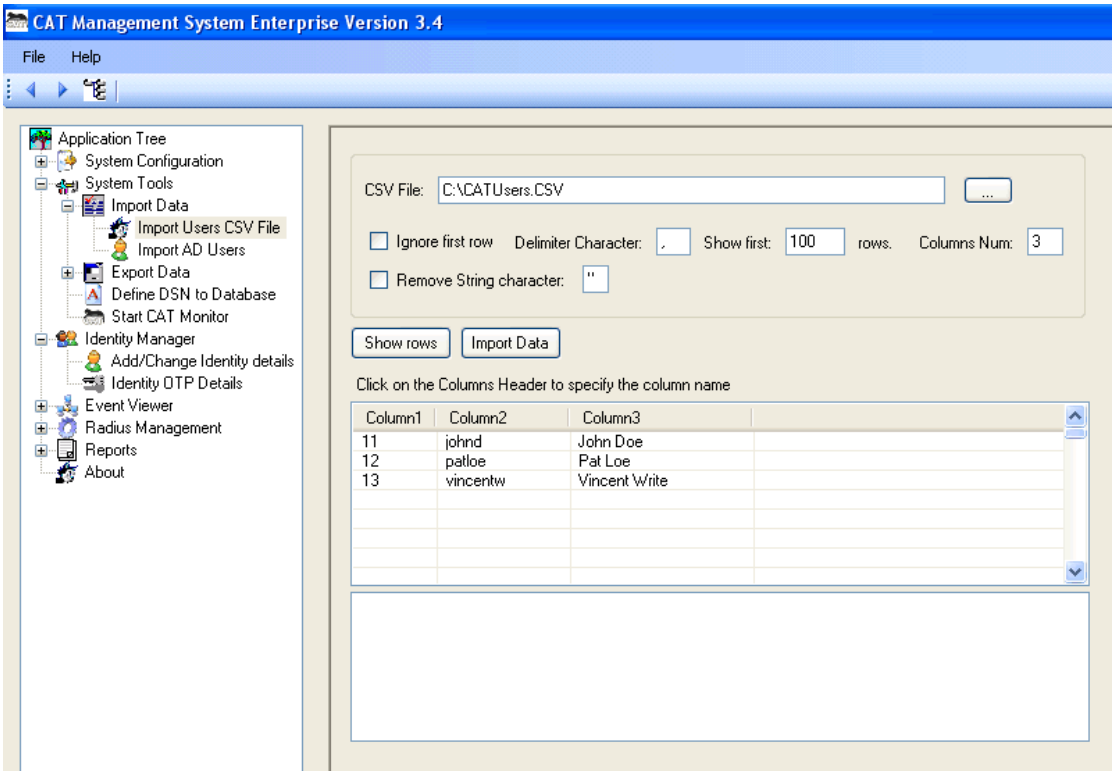
Start CAT Monitor with Windows – to start the CAT Monitor when the OS system boots.

System Tools

Import Data ➔ Import Users CSV File

The CAT MS Enterprise system allows you to import users from external sources. One source is a list of users in a typical CSV file.

The CSV file must contain at least the Login Name (User ID) and Full Name. Other information is optional.
The User Ids must be unique, or some of the users will not be imported.



CSV File - Enter (or select) the CSV file.

Ignore first row – check this option if your CSV file contains a header row. Some CSV files are created with a Columns Names row. That option will cause the Import to ignore the first row of the CSV file.

Delimiter Character – The default delimiter is: , enter the delimiter if it is other then ,

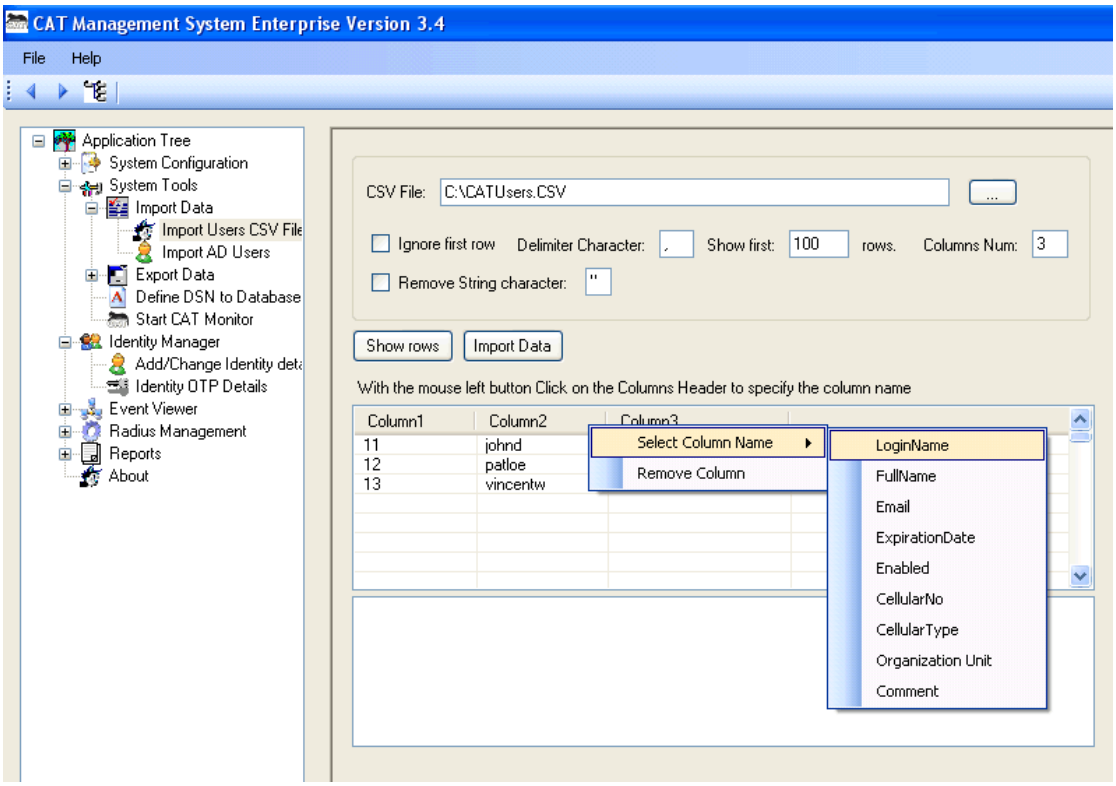
Show first XXX rows – the first stage after completing the options is to view the content of the CSV the way it will be imported. The default is to show the first 100 rows. This number does not limit the number of imported rows. All CSV rows will be imported.

Columns num – show the first XXX columns from the CSV. Those columns should include the mandatory Login Name and Full Name columns.

Remove String char – some CSV files add a character to String columns at the beginning and end of the column. The column looks like: "Arnnei"
Select to remove the " character using this option and the imported name will be: Arnnei

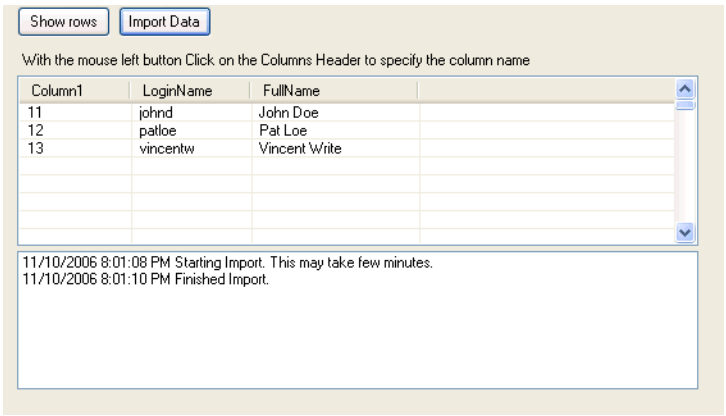
Once all the option has been set, press the Show rows.

Check the data and assign a column name to each column.
To make the assignment, click on the column header with the LEFT MOUSE button, and select the column name from the column names list.



You can select any one of the column names from the list. You don't have to assign all names, but you must assign the mandatory names. So, the minimum number of required columns – is 2.

When you have finished assigning columns names, press Import Data button to execute the import.
The Import Log will be created.



Once the import is completed, the new Identities can be viewed at the Add/Change Identity Details.

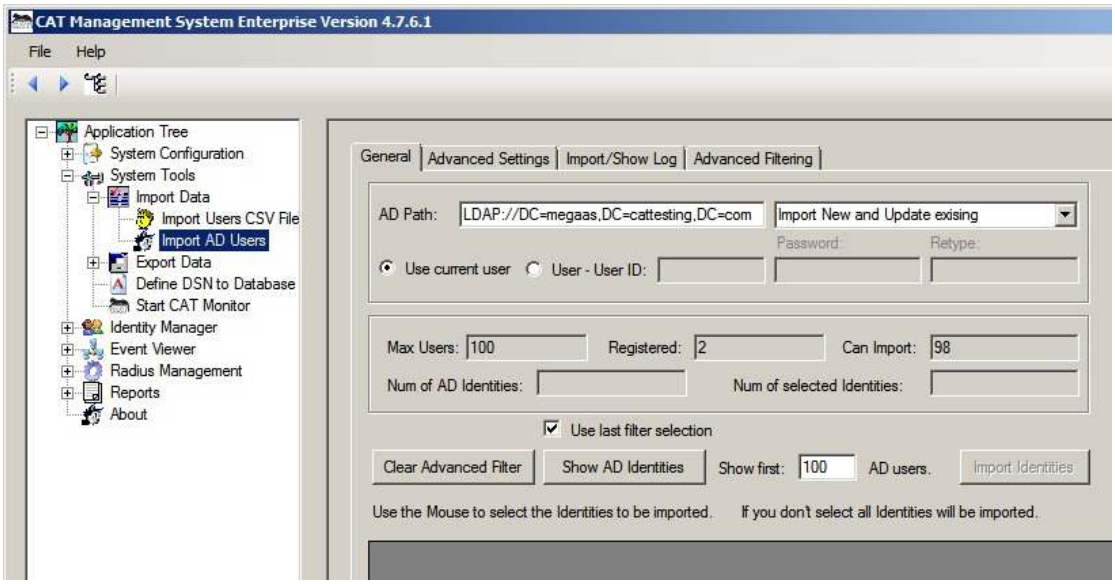
Note: If your columns did not have an Enabled column that specifies for each Identity if it is enabled or not, the system will ask whether ALL the identities are to enabled on import.

Import Data ➔ Import Active Directory Users

The CAT MS Enterprise system allows you to import users from an Active Directory.
The Active Directory can belong to same domain where the CAT is installed or it can be on another Windows Server. This option can only be used when the CAT MS is installed in a Windows Server OS.

The Import AD Users, is a onetime import action. The CAT Management System allows the administrator to customize a periodical synchronizations task. Please refer to: Configure AD Auto Sync) for further details.

Using the Import AD Users requires certain knowledge of the Active Directory structure and filtering technique to achieve a higher level of import customization.



General Tab

AD Path field – When you enter the Import AD Users form the CAT MS will try to automatically identified the Domain that you are currently working in and will create the default AD Path string for you. The Path can be changed to refer to a remote server by adding the IP address. For example:

LDAP://192.168.133.199/DC=MyDomain,DC=com

You can also use other parameters to refine the import. For example if you want to import the users of an Organizational Unit called: Management at the local domain use:

LDAP://OU=Management, DC=MyDomain,DC=com

When you are making a partial import of existing users make sure you understand the behavior of the “Disable Missing Ids” option.

Once the AD Path has been defined you have to decide the AD Import type. You choose between:

- **New Identities.** Add to the CAT MS all the Identities that are in the AD but not in CAT MS. Remember that the maximum number of registered identities in CAT is dictated by the CAT Key that you have. The system will not allow importing more then that number. The information field Max Users, Registered, Can import – show you the current statistics of how many Identities you can import. With this option you cannot use the “Disable Missing Ids” option.

- **Existing Identities.** Update the existing Identities that are in the AD and in CAT MS. Since you are updating the already existing Identities, the system will not check the Can Import information field.

- **Both.** In this case, since you are also importing new identities, the system will check that you are not running over the Maximum registered users limit as defined by your CAT key.

Use Current user or Use a different User ID/Password – Choose the credentials for accessing the Active Directory. Either use the credentials of current Windows user or enter another User ID/Password.

Max Users (information field) – The Maximum allowed registered users for your CAT AS as derived from your CAT Key.

Registered (Information Field) – The current number of Identities registered in your CAT MS.

Can import (Information Field) – the difference between the Max allowed number and the Registered number.

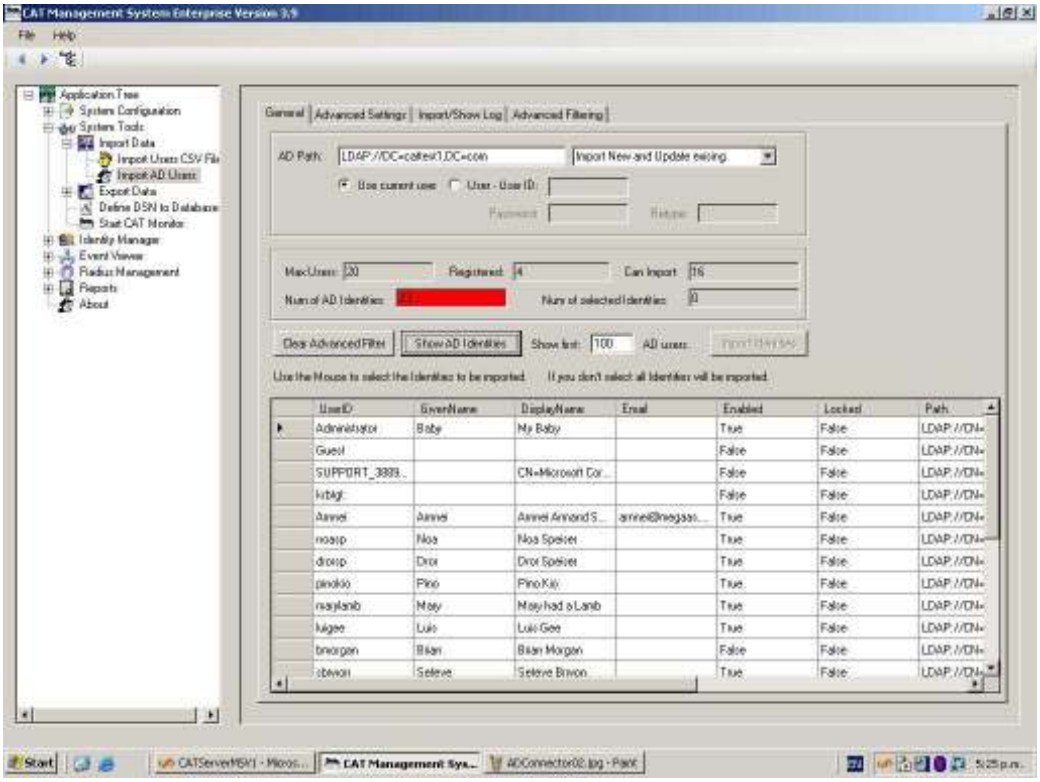
Clear Advanced Filter (Action Button) – clears all the previous selections made at the Advanced Filtering tab.

Show AD Identities (Action Button) – fetches the selected AD Identities ad shows them in the table area for inspection before import. You can limit the number of fetched Identities using the Show First field.

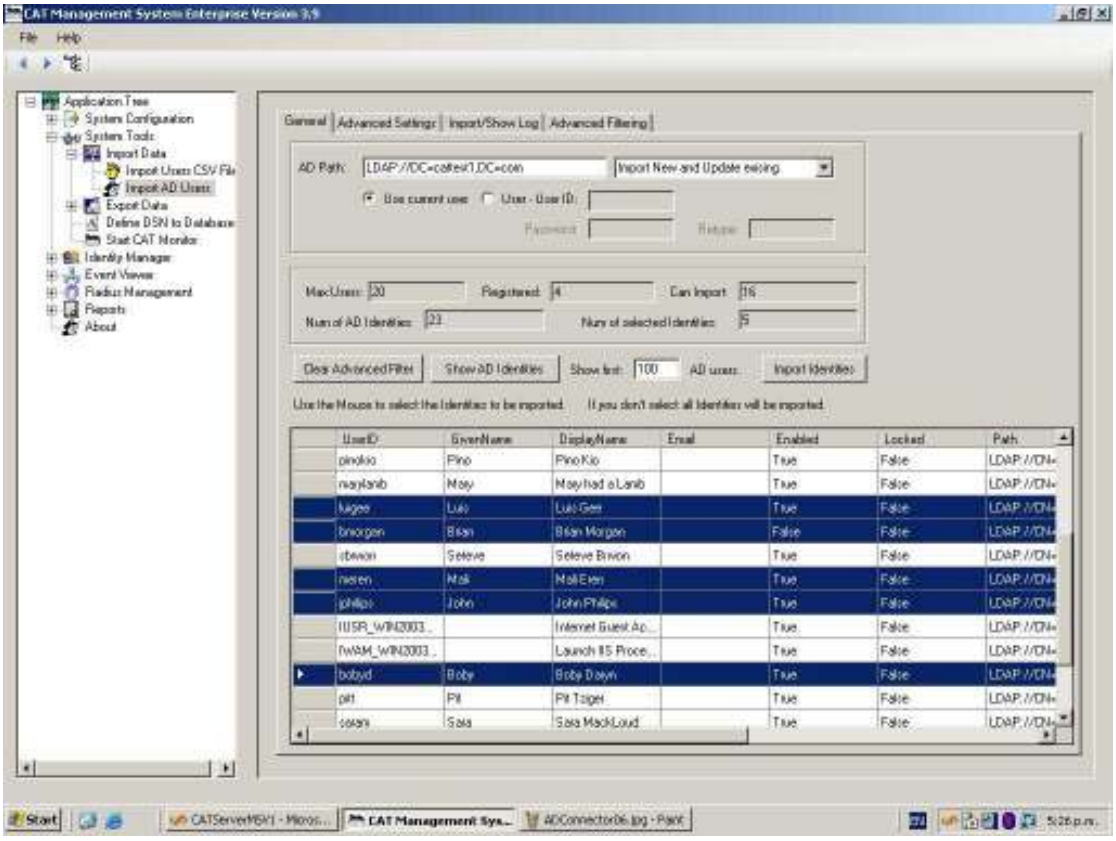
Show first XXX AD Users – This relates to the action button of Show AD Identities. Pressing the button imports the activities into the information table below. This option allows you to define how many rows you’d like to see. Enter a 0 (zero) to show all the Identities. This number has NO effect on the import action. The import always imports all the selected rows in accordance to the CAT Key limitations.

Following is the result of pressing the Show AD Identities.

You can see the results in the information AD. The Import Type selected was – New & Existing. The system found 23. The system identified that you can import only additional 16 identities, colored the Num of AD Identities in red and locked the Import Identities action button until you decide which Identity to import/Update.



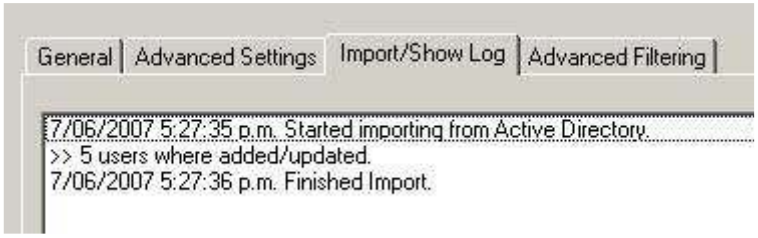
Once the Identity has been selected the red color is back to normal and the Import Identities action button is unlocked.



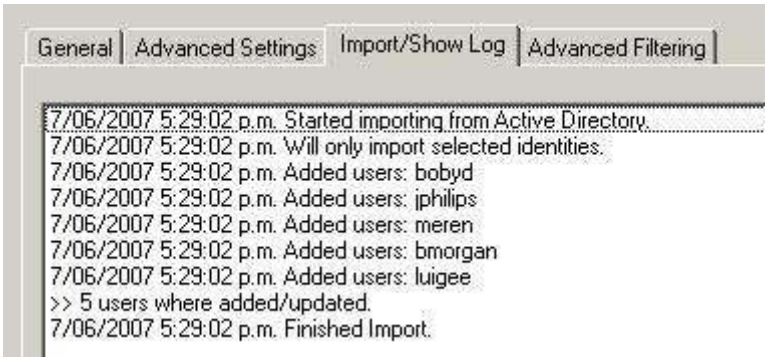
Import Identities (Action button) – executes the import from AD and inserts/updates the Identities into/in the CAT Management System.

The import log can be viewed the Import Log Tab.

Following is a normal import Log result.

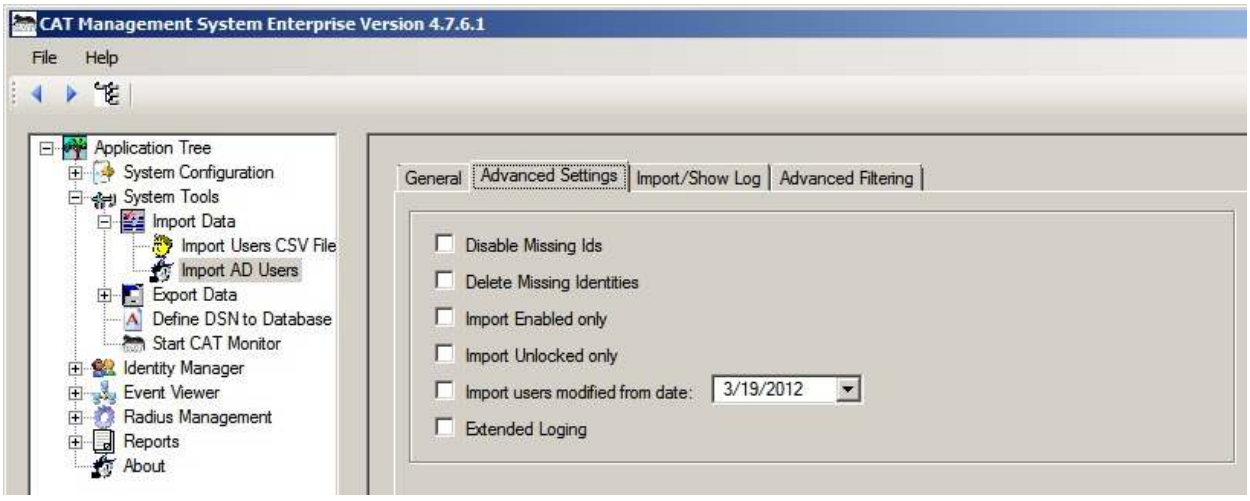


If you selected to have Extended Logging, the import Log can look like:



The log will give more information in cases an Identity was not updated.

Advanced Settings Tab



Disable Missing Ids option – This option is most useful when you are making full synchronization with the domain AD. Be cautious when you are making only a partial import of your exiting domain AD. This option is running as a second step to the AD Import. Once all

the existing users and new users have been updated in the CAT MS the system checks which Identities in the CAT MS WHERE NOT UPDATED. Those Identities are disabled.
If you are making a partial update, for example – only those activities that changed from a certain date, or only a certain Organizational Unit etc. and you choose to "Disable Missing Ids" the system will disable ALL the Ids that were not found in the selection.

Delete Missing Identities – is the same as Disable Missing Ids, only the missing Ids are removed from the CAT Management System.

Import Enabled Only - Only import identities that are enabled in the AD. Using this option in conjunction with the Disable Missing Ids is an efficient way to disable in CAT MS any Identities that were removed from the AD or were disabled in the AD.

Import Unlocked Only - Similar to the above, but only imports AD Identities that are not locked for any reason in the AD.

Import Users modified from date – Import only AD Identities that where added/modified at or after the selected date.

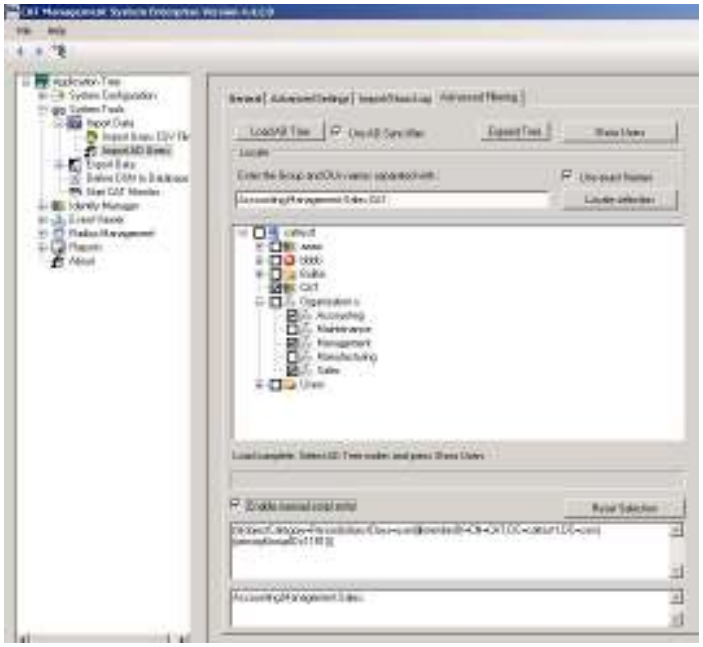
Extended log – when selected, the generated execution log includes low-level messages that refer to the way the execution was carried.

Import Log Tab

The Show AD Identities and Import buttons generate log messages regarding the performance and results of the actions.

Advanced Filtering Tab

The Advanced Filter builds the AD Organizational Units (OU) and Security Groups tree. Once the tree is built, any branch can be selected and the nested sub groups are selected as well. The selection is translated into a Filter script presented at the bottom of the window.

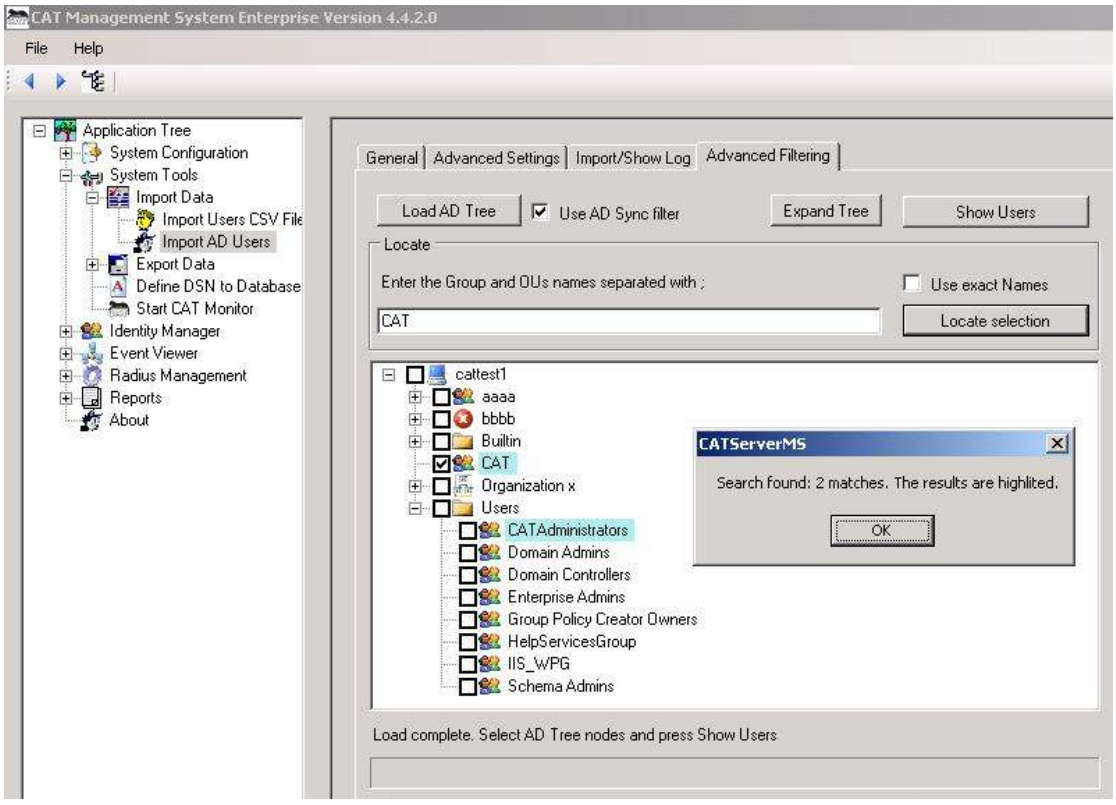


For information about the different options have a look at Advanced Filtering Tab at the Configure AD Sync option.

When loading the AD tree, in cases that AD Sync is used, the administrator may request to use the saved AD Sync filter as default by checking the Use AD Sync filter.

Once the filter has been decided the administrator can press the Show Users button to jump to the General tab and view the filter selection results.

Using the Locate Selection button marks the results by blue highlight:

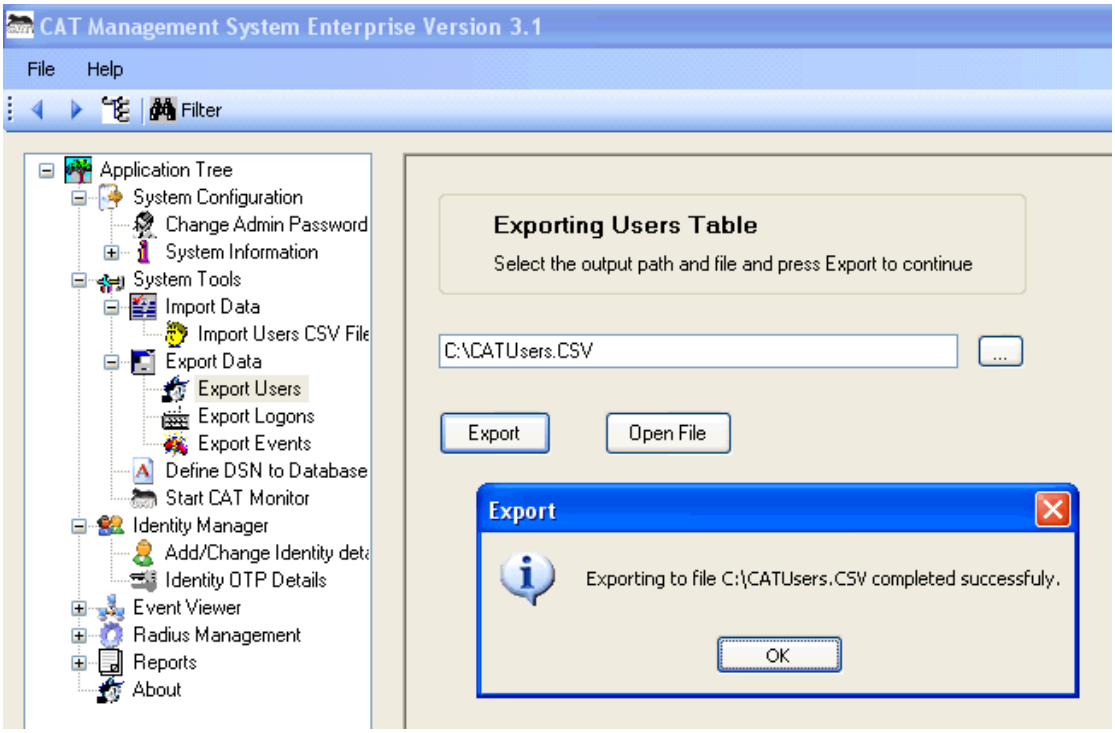


In this example the administrator was looking for all the groups and OUs that contained the string CAT. The results were 2 nodes. If the administrator was looking for the specific name CAT he could check the Use exact Names option.

Notice – the selection of Groups AND Organization Units results in the intersection sub group as explained above.

Export Data ➔ Export Users

To export the Users data, select or enter the File name and path.
Press the Export button to execute the Export and wait for the successful Export message.



To open the exported CSV file with MS Excel, press the Open File button.

Note: The CAT MS does not export – Users Secret Data or OTP.

Export Data ➔ Export Logons

To export the Logons events log, select or enter the File name and path.
Press the Export button to execute the Export and wait for the successful Export message.

Export Data ➔ Export Events

To export the Events log data, select or enter the File name and path.
Press the Export button to execute the Export and wait for the successful Export message.

Define DSN to Database

This option opens the Windows Administrator tool for defining new DSN.
Please refer to Creating a DSN.

Start CAT Monitor

If the CAT Monitor is not started, select this option to start it.
The monitor Icon will appear at the Notifications area.

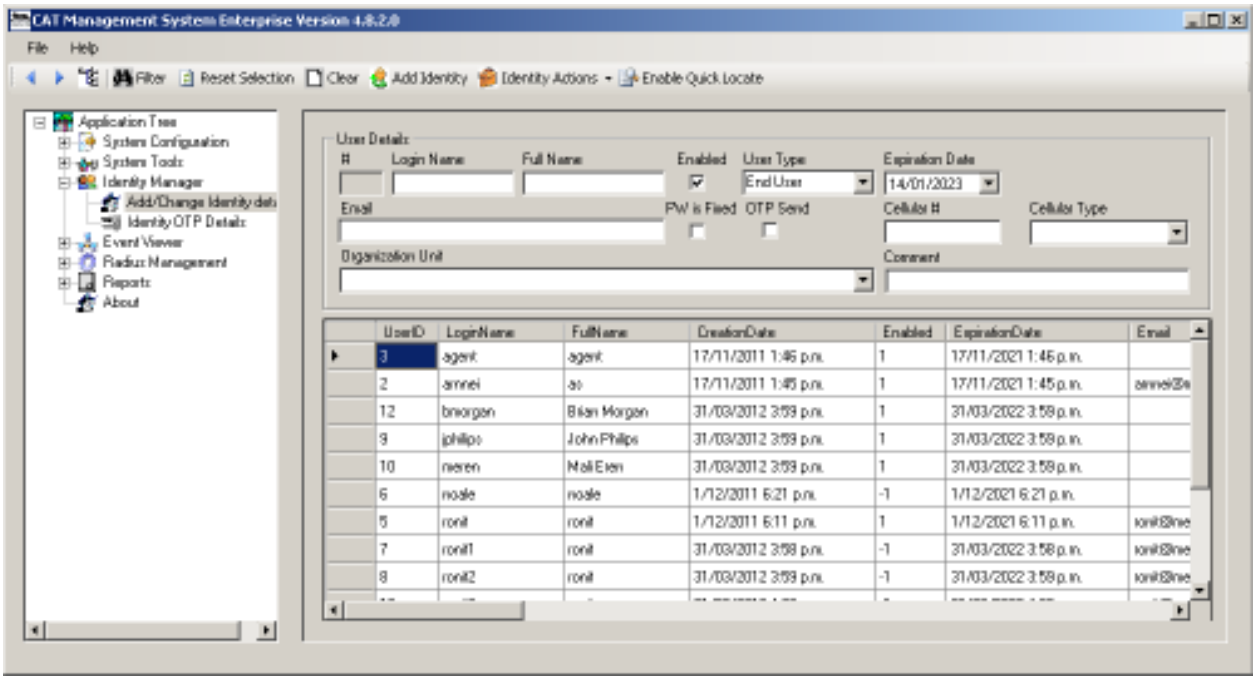
For more information about the monitor please refer to Using the CAT Monitor.

Identity Manager

Add/Change Identity Details

The Add/Change Identity Details task allows you to add manually new Identities and update existing identities details. These actions are logged in the Events log.

Each Identity has a unique User ID number that is created by the system when the Identity is added.



The administrator provides the following information fields when the Identity is added manually:

- **Login Name** – Used by the user each time he Logins to the Server. This is a unique identifier of the Identity. This Field is mandatory.
- **Full Name** – The full name of the Identity (person). This Field is mandatory.
- **Enabled** – True/False field that indicates the status of the Identity. If the Status is False, the Identity will be denied access to the Server.
- **User Type** – 3 types: End User, Support and Administrator. Administrator or Support Identity cannot Login to the Server using OTP. It can only be used to open and manage the CAT MS. An Administrator must have a Fixed Password defined.
- **Expiration Date** – Another way to control the status of the Identity. If the Expiration Date has passed, the identity will be denied access to the Server.
- **Email** – Information field. Please enter the identity Email. The system checks that the Email is valid.

- **PW is fixed** – A user can have a temporary status of Using Fixed Password for example if the user does not have access to the CAT Token. In that case, the Fixed Password is equal to the user's Secret Data. This will not be the same Secret Data as for the OTP. Each time the status of the user changes between Fixed to OTP Password, a new Secret Data is generated.

- **OTP Send** – True/False for enabling this Identity to sending Fixed Password by SMS or there delivery means. Selecting OTP send also converts the user to Fixed Password mode.

- **Cellular #** - Information field. The Identity Cellular Number. Can be used for integration with SMS systems in case this user should get SMS messages.

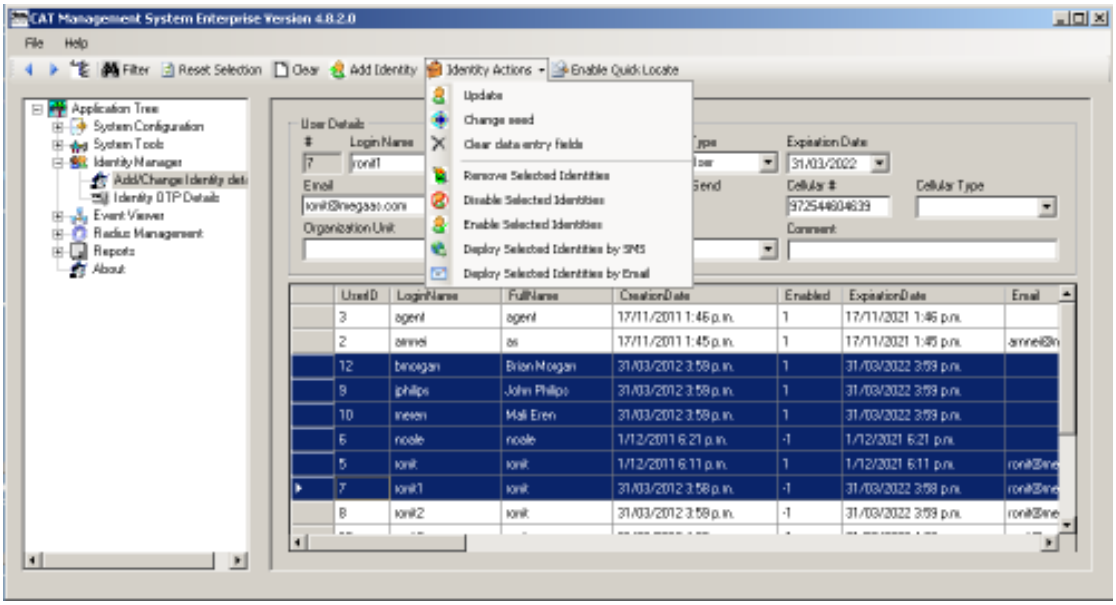
- **Cellular Type** – The Cellular manufacturer and version. Can be used for internal statistics.

- **Organization Unit** – Information field. Can be used for internal statistics.

- **Comment** – Information field. Can be used for internal statistics.

Note: Information fields are not mandatory.

The CAT MS allows the following Identity Tool Bar Actions:



Clear

Pressing the Clear button on the Tools bar will clear all the Data Entry fields.

Filter

The Filter is used to search/select groups or individual Identities.
For more information look at: Using the Data Filter

Reset Selection

Pressing the Reset Selection button on the Tools bar will reset the Filter selection and will show all the Identities.

Add Identity

Once the identity details have been entered, press the tool bar Add Identity button and the identity will be added to the database.

Update Identity

To update an existing identity, the Identity must be selected first.
When the identity is selected (point and click using the mouse left button on the gray area left of the User ID) the details of the identity are loaded into the data entry fields.

When the identity data has been changed and are ready for update, press the Update task at the Tools Bar tasks list under the Identity Action.

Clear Data Entry Fields

Clear the content of the fields from the last selected Identity details.

Change Seed

To update and identity, the Identity must be selected first.
When the identity is selected (point and click using the mouse left button on the gray area left of the User ID) the details of the identity are loaded into the data entry fields.

The Seed is not changed manually. The System will calculate a new Seed for the Identity and store it internally. A new Seed means that the Identity will have a new Secret Data.

Note: When the Seed is changed the Identity must be provided with the new seed, or it will not be able to Login to the Server.

Remove Selected Identities

To remove identities, at least one Identity must be selected first.
When the identity is selected (point and click using the mouse left button on the gray area left of the User ID) the details of the identity are loaded into the data entry fields.

Pressing the Remove Tools bar button will erase the identity from the CAT MS.

Disable Selected Identities

The Administrator can use the mouse + shift or CTRL to select groups of Identities and Disable all the selected identities.

Enable Selected Identities

The Administrator can use the mouse + shift or CTRL to select groups of Identities and Enable all the selected identities.

Deploy Selected Identities by SMS or Email

The Administrator can use the mouse + shift or CTRL to select groups of Identities and deploy all the selected identities. That option requires the "Enable CAT Deployment" at Configure CAT Deployment task to be checked.

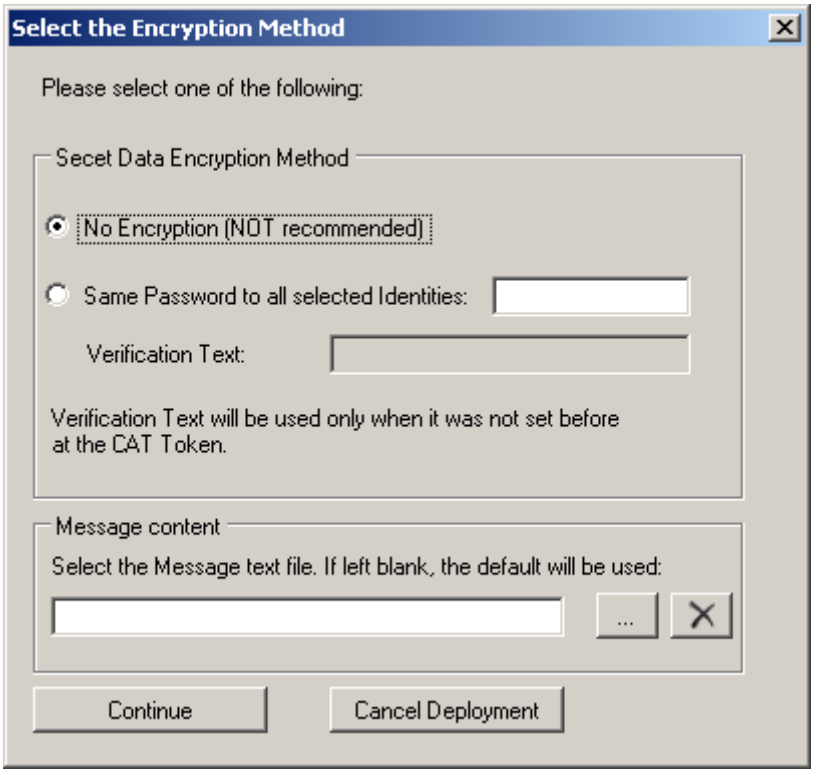
Deployment is the delivery of the CAT soft token, installation on the Cellular or Windows OS) and setting the Identity details in the CAT, to start viewing the identity OTP.

There are 2 parts in the deployment:

- Installing the CAT soft token – Installation is done like an installation of any other software on the device. Usually it will be done by downloading the software from the Internet using a link URL. This link can be keyed manually, or **sent to the cellular by SMS or Email**.

- Setting the Identity details – The setting requires 3 items (the rest are defaults). 2 of which are for information only and the third is the Secret Data (seed) that is calculated by the CAT. All 3 items has to be entered into the identity details on setup using the CAT soft token menu. The other option (available on most of the CAT soft tokens) is to **send a Set-up String to the end user (by SMS or Email) to** the end to copy and Past into a Paste field using the "Add Site by Paste" CAT menu option.

Since the Set-up string contains the Secret Data which is the basis for calculating the OTP, the administrator has an option to send the Set-up string with the Secret Data encrypted. In that case, when pasted, the CAT will request a password to open the Secret Data.



Entering a password string at the "**Same Key to all identities**" will encrypt all the Identity's Secret Data with that password. If you choose "**No Encryption**" then Secret Data will be in text format and no decryption will be required.

The Administrator has to provide the password to each of the deployed Identities/users. The password is used by the CAT Token to decrypt the Identity's Secret Data.

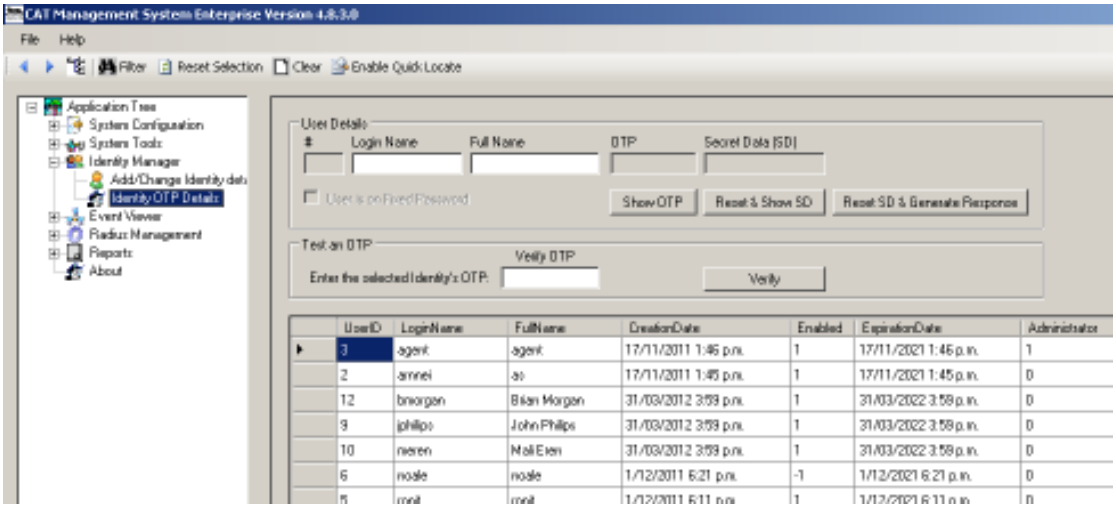
Message Content - The Administrator is able to send a pre prepared Email or SMS content to selected Identities. If a text file is not selected, the default for Email deployment or SMS will be sent.

Identity OTP Details

This task provides the administrator with the most secured details of each identity:

- The Secret Data
- Current OTP.

The task also enables the administrator to test OTP for a selected identity.



Select the Identity by point and click with the left mouse button on the selection column left to the User ID column.

The selected Identity details will be loaded to the User Details fields.
For security reasons the Secret Data and OTP are protected and not presented.

Show OTP button - to see the selected Identity's OTP the administrator ahs to press the Show OTP button. The action is logged and the current calculated OTP is presented.

Reset & Show SD button - to see the Identity's Secret Data the administrator has to press the Show Secret Data button. The action is logged and a new Secret Data is calculated and presented. The Administrator can change the settings at the System Settings task to prevent Secret Data change when viewed. The button title will change to: **Show SD.**

Reset Secret Data & Generate Response button – to open the Challenge Response window press this button. The challenge is created on the CAT Token, entered in this windows and a response is generated. The response is entered into the CAT Token to create the Secret Data.

Notice – each time the Secret Data is presented it is new. Each time the Secret Data has to be set up again on the Identity's CAT Token or the Identity won't be able to Login. Requesting to Show Secret Data or Challenge Response the secret data – generates a new secret data.

The Administrator can now deliver manually the Secret Data to the Identity, for the Identity's CAT setup.

Note: The OTP is calculated with a time counter that relates to the Server local zone. If the Identity (user) is at a different time zone, his CAT will produce a different OTP that is still

valid. To check if a particular OTP is valid enter/past it into the Verify OTP field and press the Verify button. The system will check the validity of the entered OTP.

Note: If the user is currently set to using Fixed Password, the OTP will not show. Only the Secret Data is presented and the Secret Data is currently the Fixed Password for this user.

The CAT MS allows the following Identity OTP Actions:

Filter

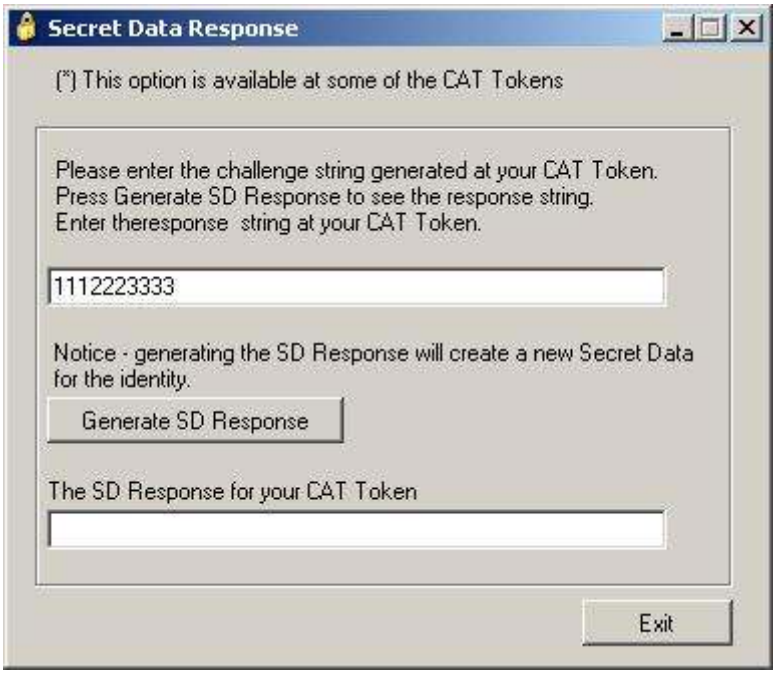
The Filter is used to search/select groups or individual Identities.
For more details look at Chapter 4 – Using the Data Filter.

Reset Selection

Pressing the Reset Selection button on the Tools bar will reset the Filter selection and will show all the Identities.

Secret Data Challenge Response

This window opens when pressing the Secret Data Response button at the Identity OTP Details form.

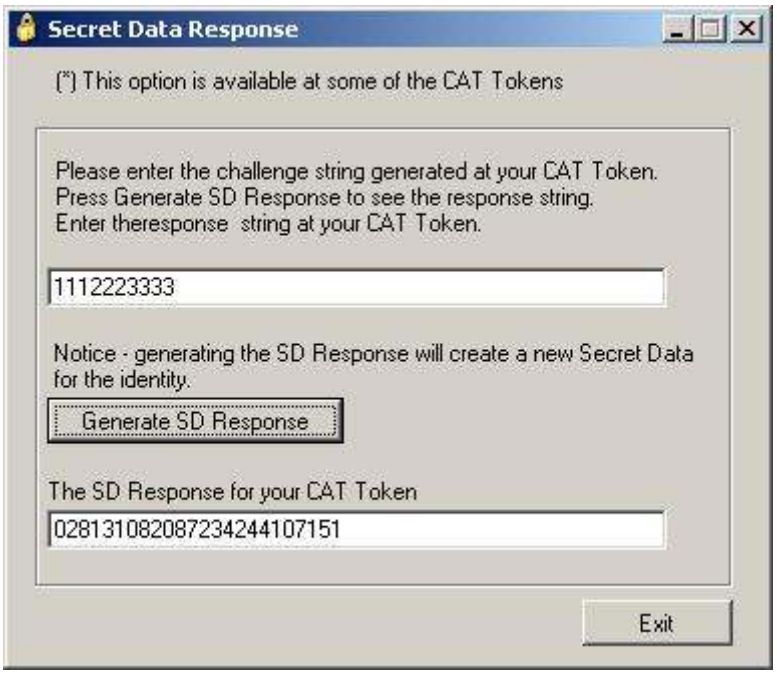


The Challenge number is generated at the CAT Token. Use the CAT Token Add Site Manually CR menu option. After entering the Site and Account details, the CAT Token presents a Challenge number.

You can find the CAT Token Challenge Response form images at Mega AS web site: www.megaas.com

Press the Generate SD Response button to generate the SD Response number.

Notice – when you generate the SD Response, you are also generating a new Secret Data. You'll be prompted with a message to confirm the step.



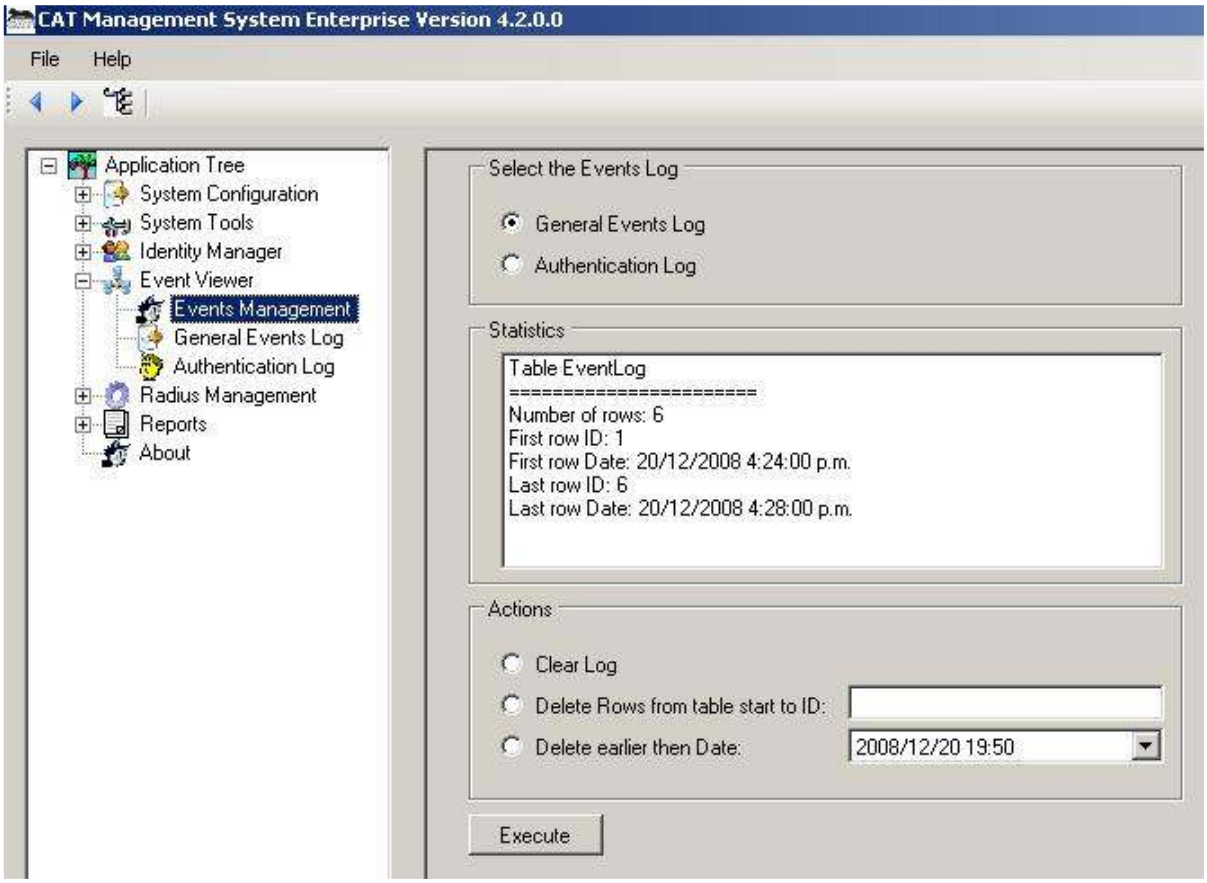
Enter the generated SD Response number at the CAT Token response field and press OK to complete the setting of the Site / Account at the CAT Token.

Events Viewer

Each of the Administrative actions are logged at the Events logs.
There are two different logs contents.

Events Management

The Events Management is a utility for cleaning the Log tables.



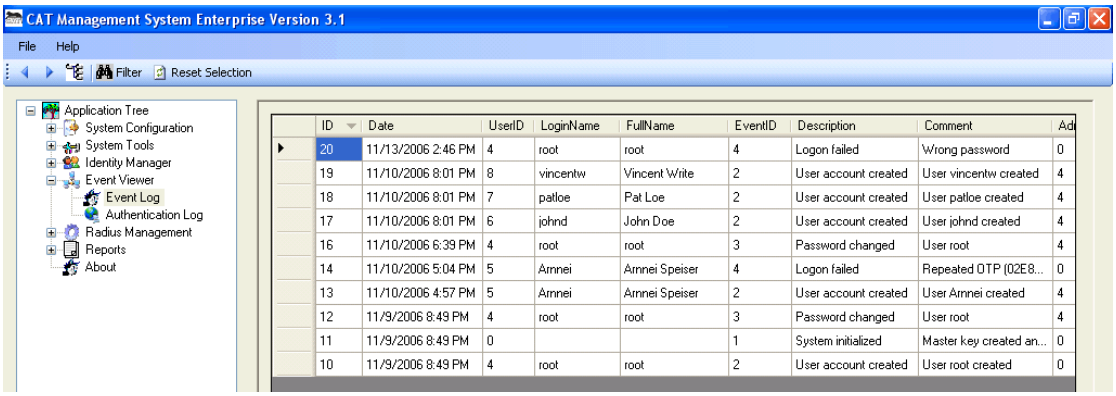
The Administrator can “Select the Event Table”. When the table is selected the statistics box shows basic information regarding the Log table. That is formation can help deciding if and how many rows to delete from the table.

The following Actions are possible for each of the tables:

- Clear table – clears all the rows.
- Delete rows from table start to ID – Each Log row has an ID number. The ID is presented in the Log views. This action will erase all the rows up to the entered ID.
- Delete earlier then date – delete from the Log table all the event rows prior to the selected date.

Event Log

The Event Log displays every event but the successful Logins events.



ID	Date	UserID	LoginName	FullName	EventID	Description	Comment	Ad
20	11/13/2006 2:46 PM	4	root	root	4	Logon failed	Wrong password	0
19	11/10/2006 8:01 PM	8	vincentw	Vincent Write	2	User account created	User vincentw created	4
18	11/10/2006 8:01 PM	7	patloe	Pat Loe	2	User account created	User patloe created	4
17	11/10/2006 8:01 PM	6	johnd	John Doe	2	User account created	User johnd created	4
16	11/10/2006 6:39 PM	4	root	root	3	Password changed	User root	4
14	11/10/2006 5:04 PM	5	Arnnei	Arnnei Speiser	4	Logon failed	Repeated OTP (02E8...	0
13	11/10/2006 4:57 PM	5	Arnnei	Arnnei Speiser	2	User account created	User Arnnei created	4
12	11/9/2006 8:49 PM	4	root	root	3	Password changed	User root	4
11	11/9/2006 8:49 PM	0			1	System initialized	Master key created an...	0
10	11/9/2006 8:49 PM	4	root	root	2	User account created	User root created	0

The Log can be sorted (by pressing on the column headers) and/or filtered by using the Filter.

For producing built-in reports refer to Chapter 3 – Reports tasks.

To produce personalized reports, you can export the information using the System Tools export options and use MS Excel or other reporting tools to open the CSV file and customize a report.

The CAT MS allows the following Event Log Actions:

Filter

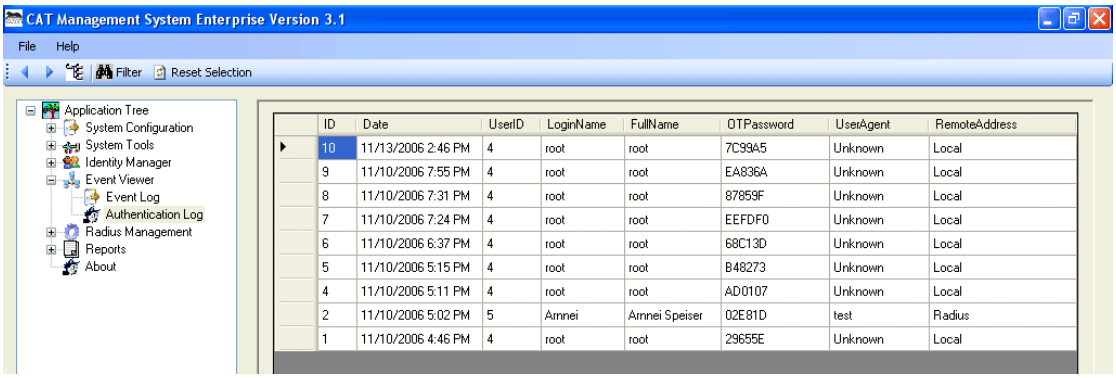
The Filter is used to search/select groups or individual events.
For more details look at Chapter 4 – Using the Data Filter.

Reset Selection

Pressing the Reset Selection button on the Tools bar will reset the Filter selection and will show all the events.

Authentication Log

The Authentication Log displays only the successful Logins events.



The Log can be sorted (by pressing on the column headers) and/or filtered by using the Filter.

For producing built-in reports refer to Chapter 3 – Reports tasks.

To produce personalized reports, you can export the information using the System Tools export options and use MS Excel or other reporting tools to open the CSV file and customize a report.

The CAT MS allows the following Event Log Actions:

Filter

The Filter is used to search/select groups or individual events.
For more details look at Chapter 4 –Using the Data Filter.

Reset Selection

Pressing the Reset Selection button on the Tools bar will reset the Filter selection and will show all the events.

Radius Management

The Radius Management is available only when the Radius was enabled through the CAT Initiation – Step 3. Using the Radius Management the administrator can:

- Manage the Radius settings – Clients, Port, Log file
- Start/Stop the Radius Server
- Debug and test the Radius server

The CAT Radius supports PAP protocol.

Configure Radius

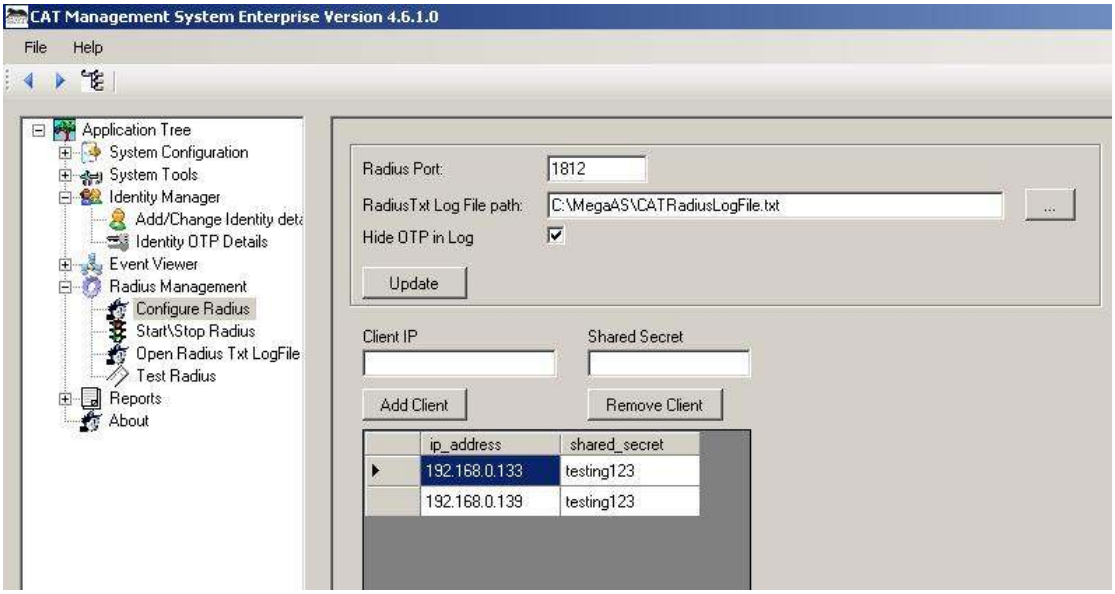
Use this option to add/change Radius clients and/or modify the Radius Server port.

For more information refer to: Configuring the CAT Radius Server

Start/Stop Radius

The Radius Server is started automatically on boot by a Windows OS Service.

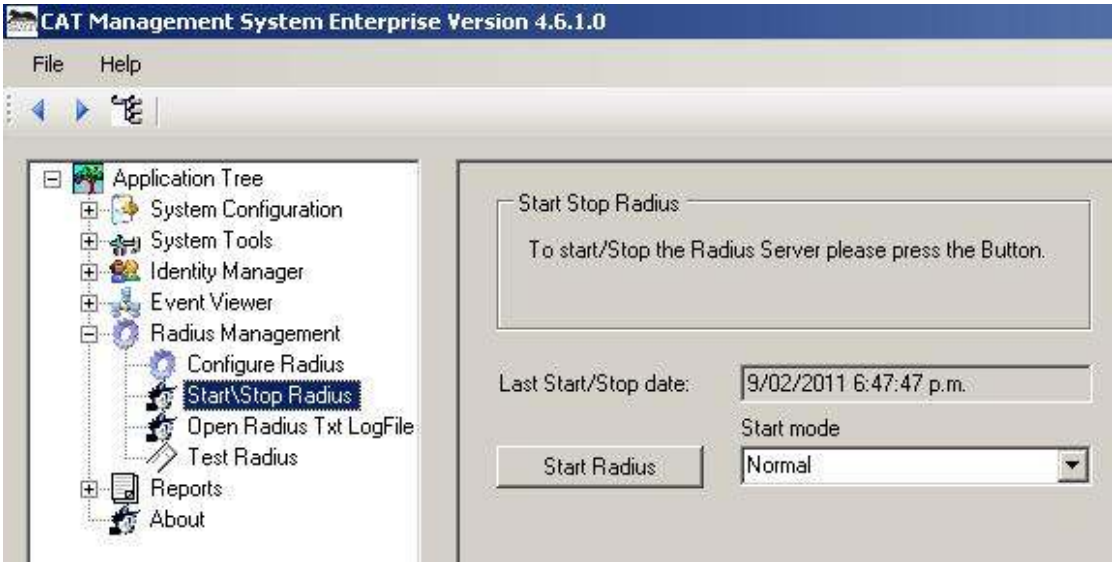
Use this option to Start or Stop the Radius Server.



To stop the Radius Server press the **Stop Radius** button.

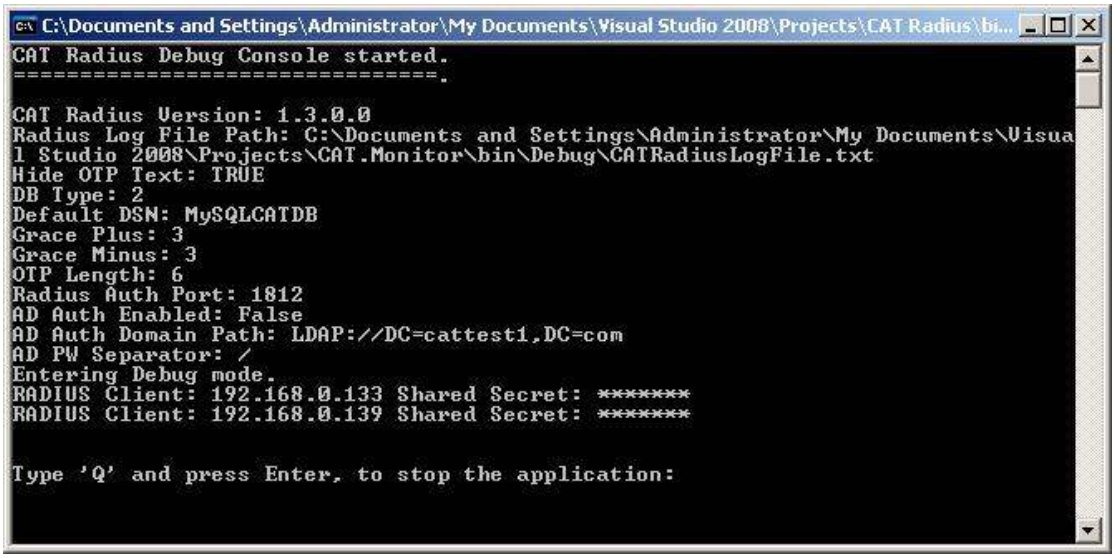
If the CAT Monitor is running, the CAT Monitor Icon will change to have a red line:

To start the Radius Server you can either use the CAT Monitor, or you can use the Start Radius button.



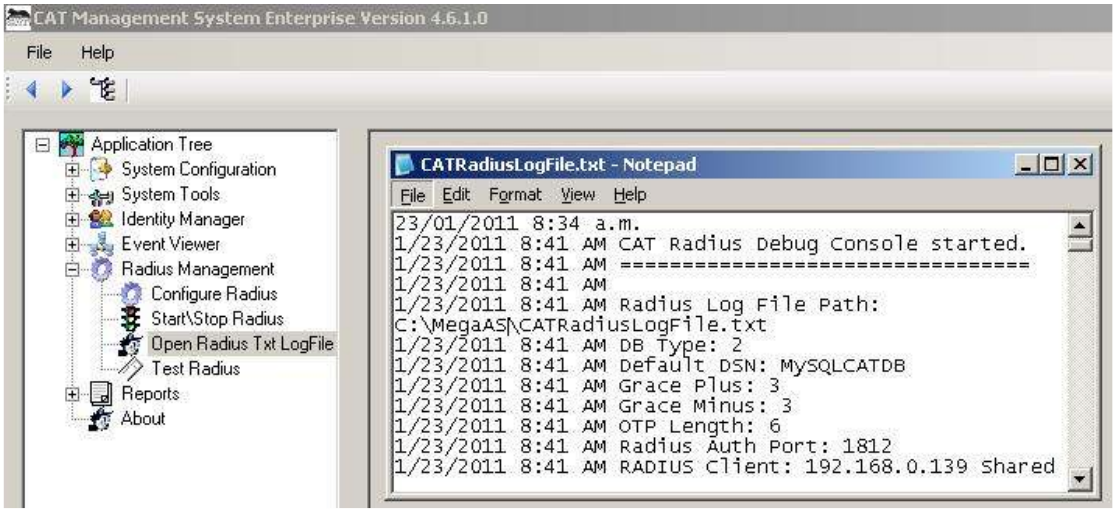
You can choose to start the Radius in the default Normal mode, or you can choose to start the Radius in a Debug mode.

When the Radius Server is started in a debug mode, a system window is opened where the Radius Server logs its internal messages for debugging purpose. Using this window the administrator can check the logic behind certain clients' requests being accepted or denied.



Open Radius Txt LogFile

This option is provided opens the Log File using the system default txt files editor.



Test Radius

This option is provided for the administrator to check the Radius Server at the end of the CAT MS installation. Please refer to
The Monitor shows the status of the CAT services by a message and color.
It will color red the message if the service is not running and green if it is running.

If the CAT is not installed with AD Sync, the related options will not be available in the monitor menu.

Start CAT Radius in Normal Mode – the CAT Radius service will be restarted.

Start CAT Radius in Debug Mode – the CAT Radius service is stopped and the CAT Radius program is started in a debug mode. A console window will open and all the system messages will be printed in the console. The messages will also be written to the text Log File if you have entered a file path.

Stop CAT Radius – will stop the current running CAT Radius.

Manage Radius Clients – opens a quick window for adding or removing clients. For the changes to take affect the CAT Radius has to be restarted.

Set Radius Port - opens a quick window for changing the port number. For the change to take affect the CAT Radius has to be restarted.

Set Radius Log File Path Clients – opens a quick window for entering or changing the Log File path. For the change to take affect the CAT Radius has to be restarted.

Open Radius Log File – opens the text file as entered in the Log File path.

The following option will be visible if the AD Sync was enabled during the installation in Initiation – Step 3. The AD Sync had to be configured using the CAT Identity Management system.

Run CAT AD Sync now – if the AD Sync is enabled, this option will start the service and cause a soon as possible run of the AD Sync.

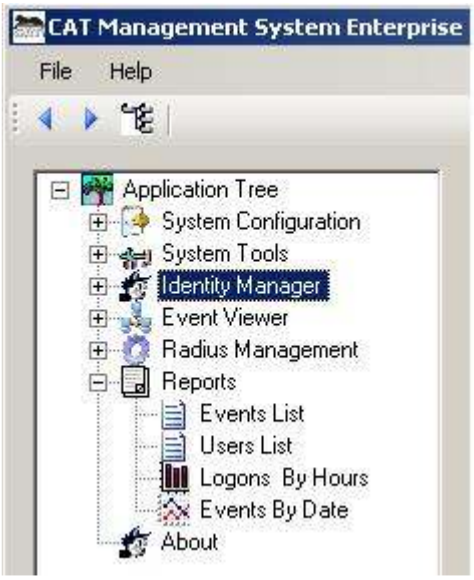
Stop AD Sync – will stop the service.

Open AD Sync Log File – opens the AD Sync Log File as defined in the CAT Identity Management system.

Testing the CAT Radius Service .

Reports

CAT MS Enterprise includes a number of default report formats.

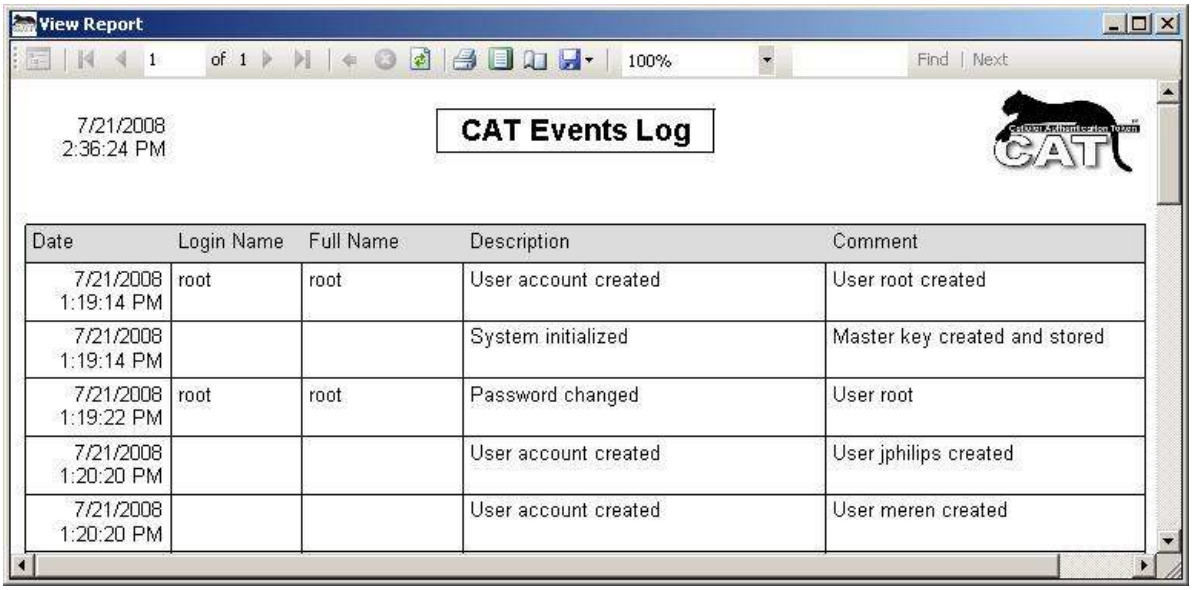


Combined with the Filter option they provide a strong Reporting tool.

When a Report format is selected, the CAT MS opens automatically the Data Filter option allowing you to select the Report records using a GUI or making advanced selections and sorting using SQL sentences.

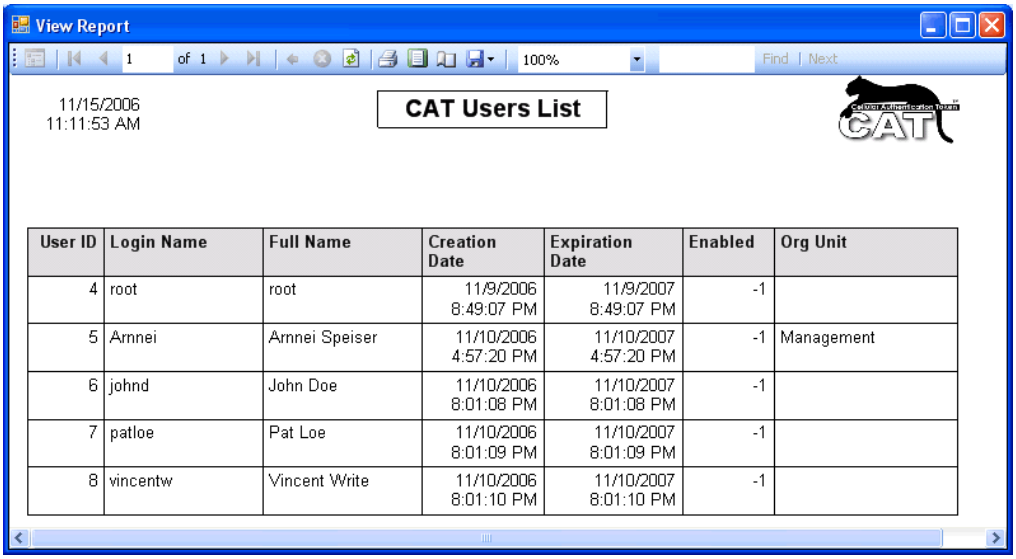
For more information about the Data Filter refer to: Chapter 3 – Using the Data Filter.

Events List



Date	Login Name	Full Name	Description	Comment
7/21/2008 1:19:14 PM	root	root	User account created	User root created
7/21/2008 1:19:14 PM			System initialized	Master key created and stored
7/21/2008 1:19:22 PM	root	root	Password changed	User root
7/21/2008 1:20:20 PM			User account created	User jphilips created
7/21/2008 1:20:20 PM			User account created	User meren created

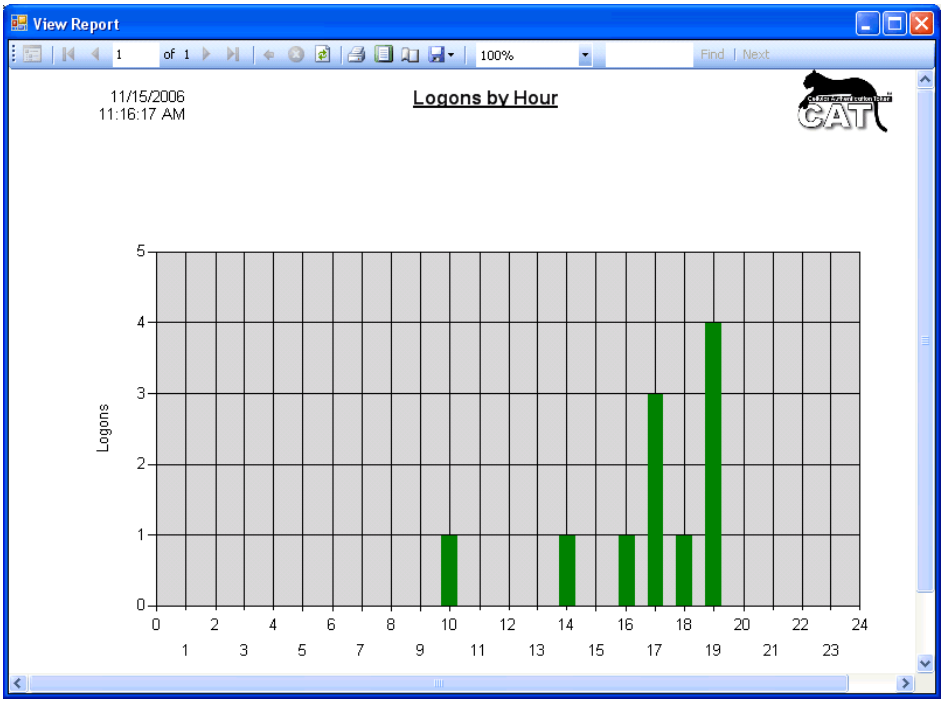
Users List



User ID	Login Name	Full Name	Creation Date	Expiration Date	Enabled	Org Unit
4	root	root	11/9/2006 8:49:07 PM	11/9/2007 8:49:07 PM	-1	
5	Arnnei	Arnnei Speiser	11/10/2006 4:57:20 PM	11/10/2007 4:57:20 PM	-1	Management
6	johnd	John Doe	11/10/2006 8:01:08 PM	11/10/2007 8:01:08 PM	-1	
7	patloe	Pat Loe	11/10/2006 8:01:09 PM	11/10/2007 8:01:09 PM	-1	
8	vincentw	Vincent Write	11/10/2006 8:01:10 PM	11/10/2007 8:01:10 PM	-1	

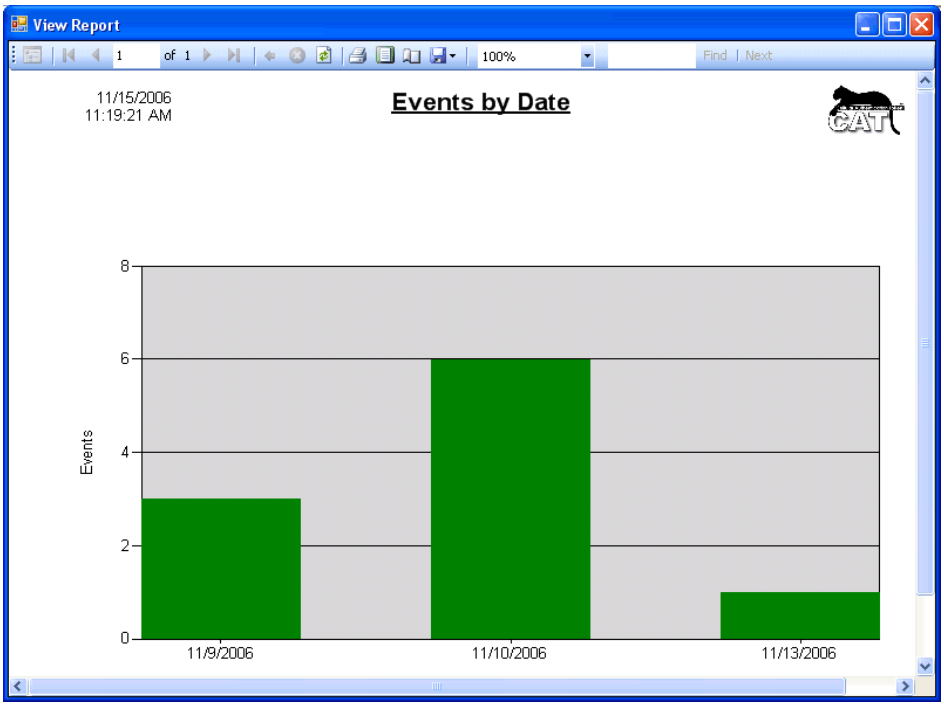
Logons by Hours

Distribution of the selected records from the Authentication Log by the time of the logon.



Events by Date

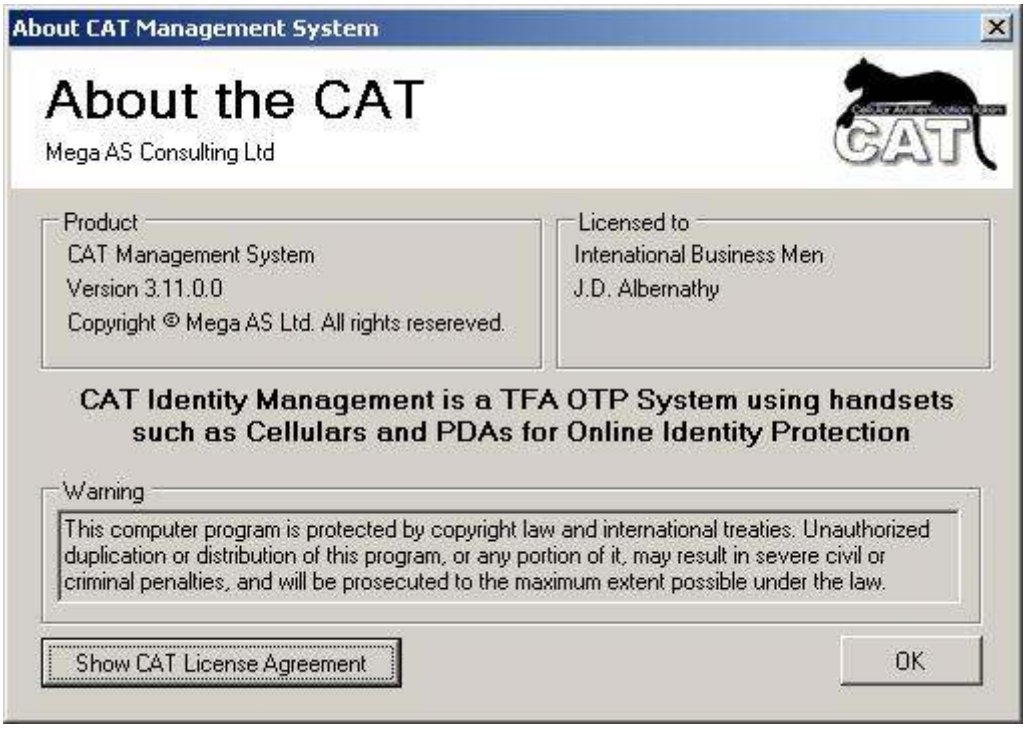
Distribution of the selected records from the Events Log by the event date.



About

CAT MS About window provides few information details about the CAT AS and an access to the CATMS License Agreement.

When the CAT MS is installed the administrator is required to read and accept the CAT License Agreement prior to completing the installation and starting to use the system.



Chapter 4 – CAT Web Services

General Description

The CAT API Web Services are a set of methods that enable calls to the CAT AS to perform certain tasks through the Internet / Intranet. It also enables certain requests to come from the Internet to the CAT AS.

The Web Services tasks' categories are:

- Existing users' tasks:
  - Authenticate Identity
  - Request automatic deployment of user's Account.
  - Request an OTP to be sent to the user by SMS or other delivery means as setup by the administrator
- New Users (Registering at the enterprise Web Site):
  - Request to register as CAT user and deploy the new Account
  - Import the deployed Account details to the CAT Cellular Token from the Internet
- General:
  - Query the server time
- Administration Tasks:
  - Enable / Disable / Remove identities
  - Show SD for selected identity

Installation and customization

The services are installed on a Windows Serve. For enhanced security use the IIS to configure the CAT AS API Service is to be accessible to only enterprise Web Site. SSL can also be used with the Web Services.

The services installation package can be found at the following folder:

Installing the CAT API Web Service (Optional)

Once the service is installed, you have to configure the CAT AS to enable the service:

Customize Web Services

Web Services methods

Table of CAT API Web Service methods:

Method	Description
AdminDeleteIdentity	Used to delete an Identity. The identity is removed from the CAT AS. Method parameters: *String strAdminLoginName* – LoginName such as root. Must be an administrator. *String strAdminPassword* – Identity password *String strDeleteLoginName* – LoginName of the identity to be removed. *String strServicePassword* – The service password as defined in the Customizing Web Services option.
AdminDisableIdentity	Used to disable an Identity. The identity stays listed in the CAT AS. Method parameters: *String strAdminLoginName* – LoginName such as root. Must be an administrator. *String strAdminPassword* – Identity password *String strDisableLoginName* – LoginName of the identity to be disabled. *String strServicePassword* – The service password as defined in the Customizing Web Services option.
AdminEnableIdentity	Used to enable an Identity that was disabled earlier. Method parameters: *String strAdminLoginName* – LoginName such as root. Must be an administrator. *String strAdminPassword* – Identity password *String strEnableLoginName* – LoginName of the identity to be disabled. *String strServicePassword* – The service password as defined in the Customizing Web Services option.
AdminGetIdentitySD	Used by an administrator to get an Identity Secret Data. Method parameters: *String strAdminLoginName* – LoginName such as root. Must be an administrator. *String strAdminPassword* – Identity password *String strLoginName* – LoginName of the identity that will return the SD. *String strServicePassword* – The service password as defined in the Customizing Web Services option.
GetCATToken	Used by the Get CAT ASP page for downloading the SMS deployed personal CAT to the cellular.

QueryClock	Returns the CAT AS Server time: yyyyMMddhhmm It can be used by the Enterprise Web Service to show the current CAT AS Server time. This way, the users can make sure their Cellular's time matches the Server time. Only the minutes has to be matched.
RegisterNewUser	Add a new Identity to CAT AS and deploy the account data to the user. Method parameters: *String LoginName* - a unique new LoginName (User ID) for the new identity. *String FullName* – The user full name. *String Email* – The user Email. *String Cellular* – The user cellular phone number. *String EcryptPW* – A password that will be used to encrypt the deployed CAT token when SendCAT option is used. *String ServicePassword* - The service password as defined in the Customizing Web Services option. *String SendCAT* – Must have one of the following values: • Donotsend • byEmail • bySMS. Sends a deployment url to the Email or Cellular number of the new Identity. For more details about the SendCAT option for easy deployment read the More about easy deployment chapter.
RequestSDResponse	Generating an Encrypted Secret Data in response to the end user CAT challenge. This is another secured option for providing the end user an encrypted Secret Data (only numbers) for adding a CAT new site, using the CAT Menu. This option is not available on all CAT tokens. Method parameters: *String LoginName* – LoginName of the requesting identity *String EcryptPW* – The challenge number as displayed on the CAT Token of the requesting identity. The response is entered in the CAT Token form and translated into the SD of the identity.

RequestSendOTP	Once the user is authenticated, he can receive an OTP (by SMS or other means) as a second factor authentication to predefine cellular number or Email etc. It is to be used **AFTER** the user has been authenticated by another method, for example – a fixed password. *String LoginName* – LoginName of the identity that the SMS is sent to. *String ServicePassword* - The service password as defined in the Customizing Web Services option. *String OTPRequestPassword* – not required.
VerifyOTP	Used to Authenticate an Identity. User enters his User Id and OTP (or Fixed Password). *String UserID* – The LoginName of the identity to be authenticated *String OTP* – The authenticated one time password generated by the CAT Token *String ServicePassword* - The service password as defined in the Customizing Web Services option.

Using the CAT Web Services

The CAT Web Services are Microsoft .Net based and can be called by any scripting language.

You can find a full

CAT Templates

To install CAT Templates open the:
C:\MegaAS\CATManagementSystem\WebServices\CATTemplates folder and run the:
CATTemplatesInstaller.msi

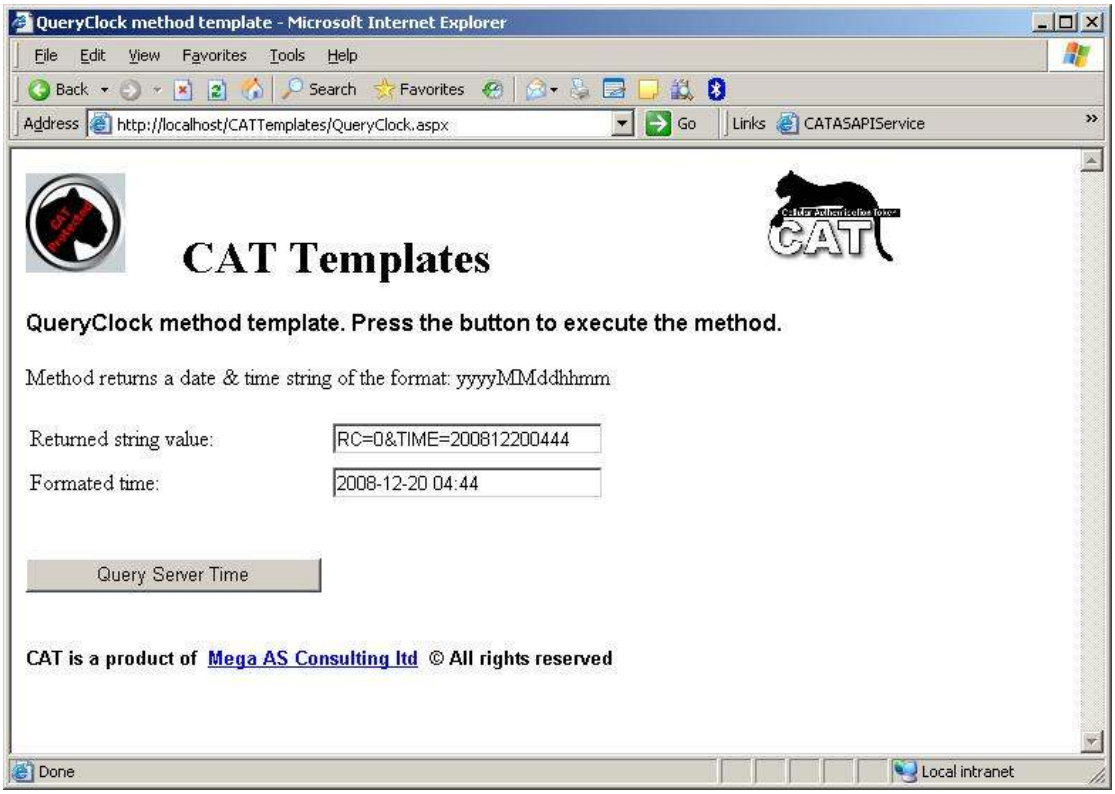
The installation includes the source code of the ASP.NET web site.
After installation, check the web.config file. Some of the API services require a service password. This password is set in the Web Services Configuration option and has t be updated in the web.config file.

If the API Services are enabled you'll be able to open and use the CAT Templates pages.

The CAT Templates Menu page

This page is the access to the listed pages, each page demonstrating the use of another API method.

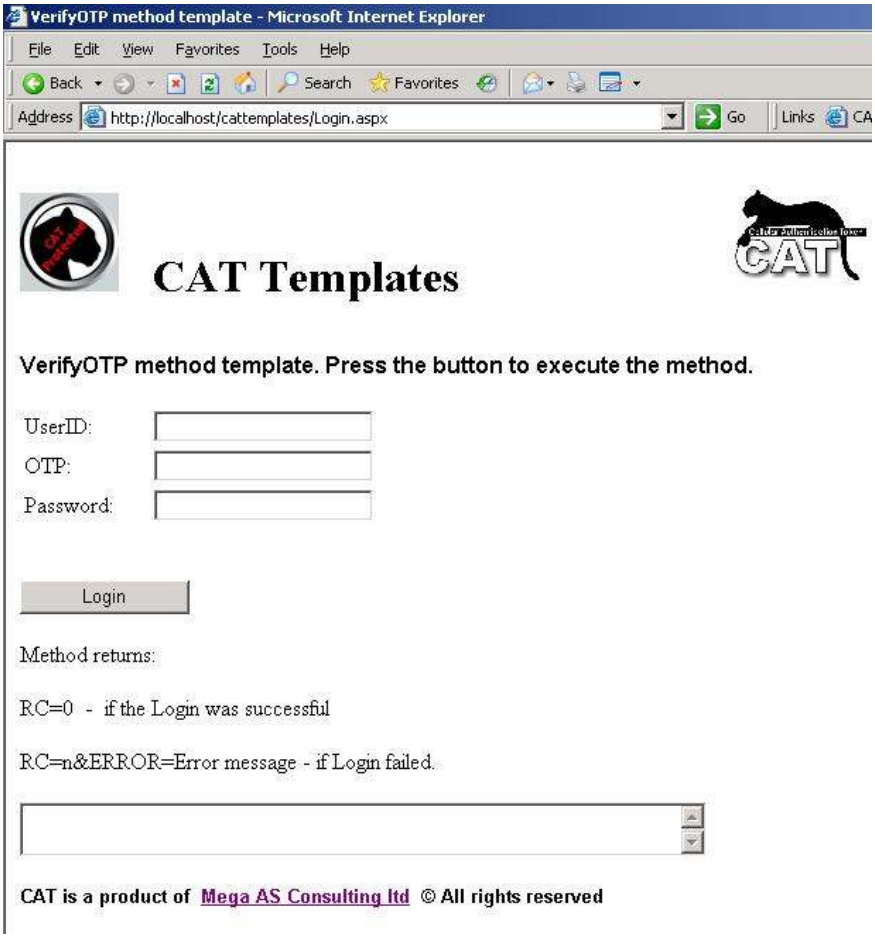
The Query Server Clock template



In this page, you press the Query Server time button.

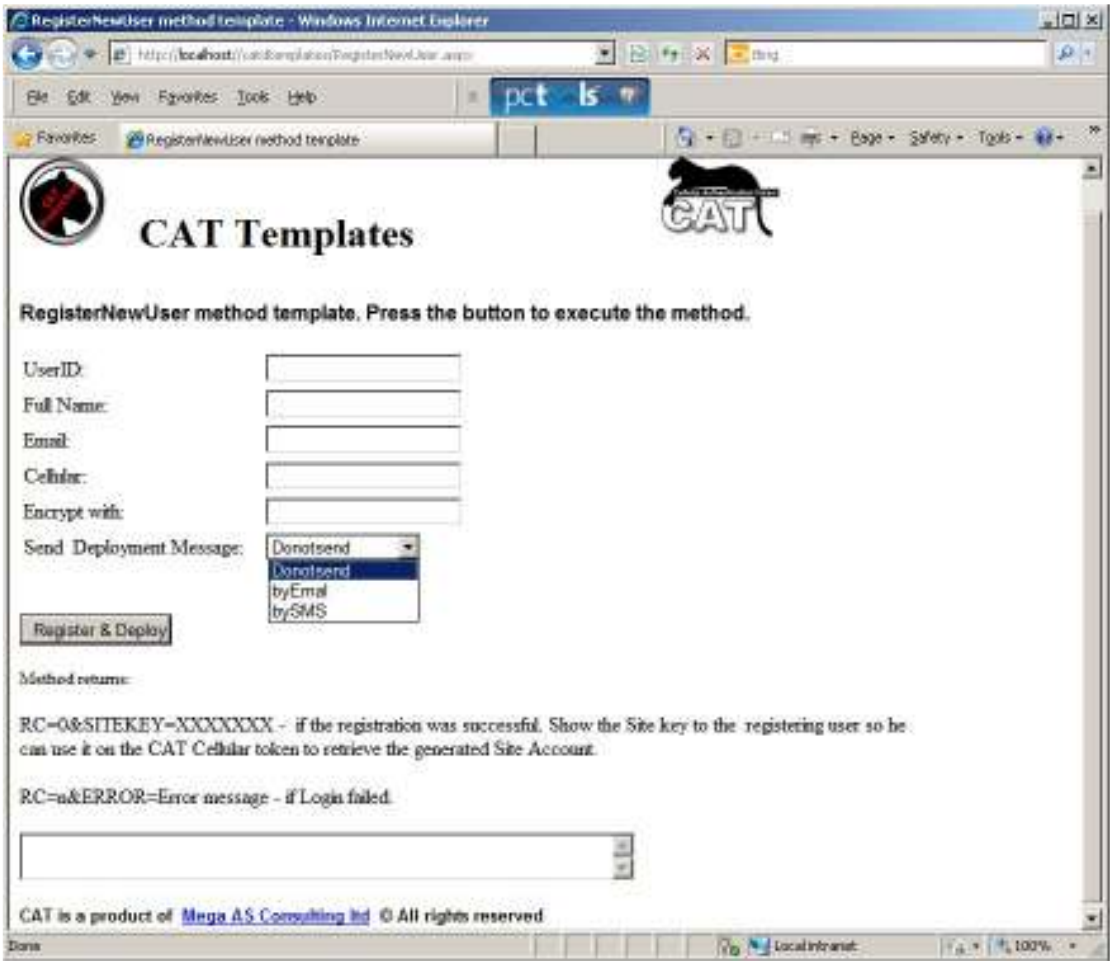
The Query Clock method is performed and the time string is returned.

The Login Template



In this page enter the identity User ID, OTP and Password (if it has one – only administrator and support have fixed passwords in the CAT).
Press the Login. VerifyOTP method is performed and success or failed result is returned.

The Register New User Template

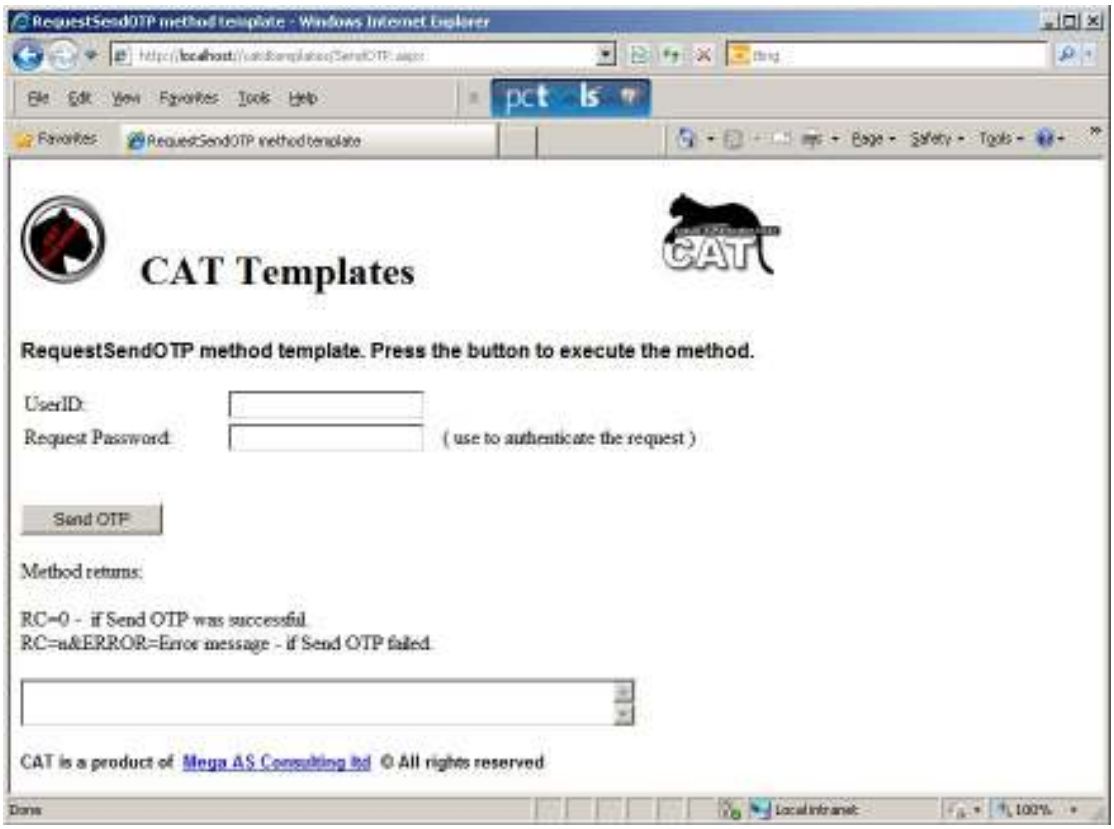


The RegisterNewUser method is used to open a new user in the CAT Management System. This method should be enabled at the Customize Web Services by checking the **Enable External Registration**.
The Method creates a new User ID with Full Name, Email, and Cellular Number.

If the **SMS CAT Token to deployed Identities** option in Customize SMS Services is checked and a Cellular Number was entered then a link to the CAT is sent by SMS to the identity. The sent CAT contains the user's Secret Data. Enter a password into **Encrypt with** field if the information is to be encrypted.
The **Service Password** is your SMS Service password when you are using the Mega AS SMS Service. It is not required if you are using your own SMS provider.

Notice – Encrypting the SD is detected by selected CAT tokens. Make sure your end user has one of those.

The Send OTP Template

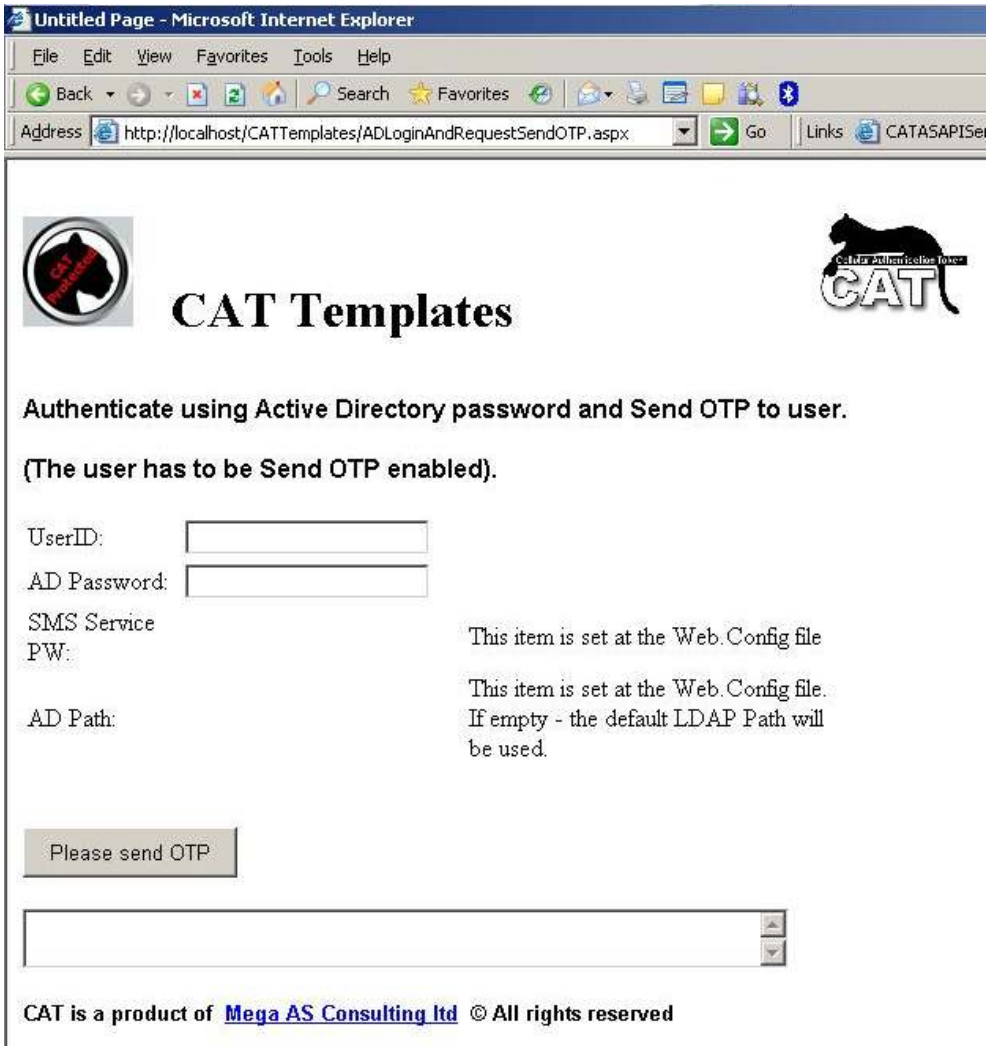


The SendOTP method is used to send by SMS an OTP to the Identity's predefined Cellular number.

This method should be enabled at the Customize Web Services by checking the **CAT AS API Service** and the **Enable SMS Passwords Service** option in Customize SMS Services has to be checked.

The **Request Password** field is for your application to verify the identity of the end user before sending the OTP. This could be an Active Directory password (see next template) or it could be another database password etc.

Active Directory authentication and SMS OTP

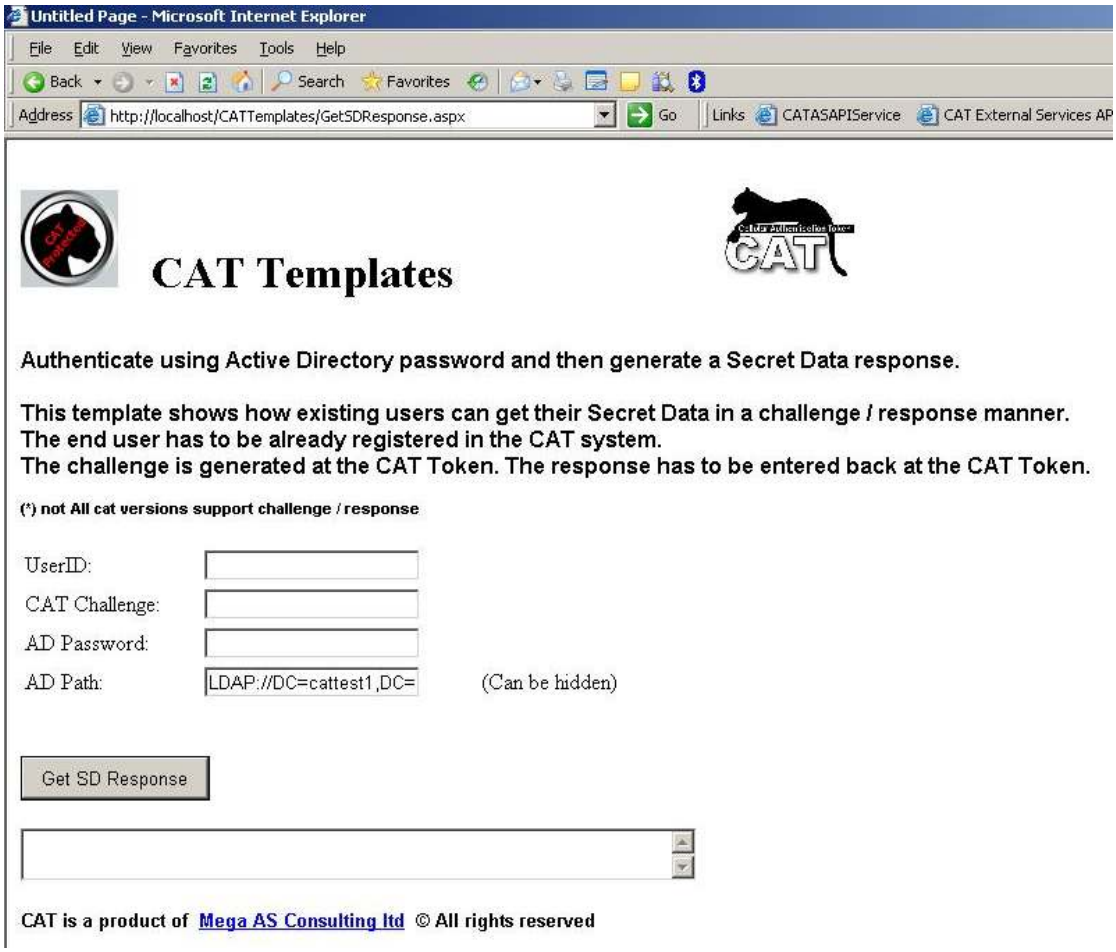


This template includes sample code for Active Directory authentication and using the RequestSendOTP method.

UserID – is the Active Directory user id.
AD Password – is the Active Directory Password of the User ID.
The SMS Service password and the LDAP Active Directory Path has to be set in the Web.Config file:
<add key="ldapPATH" value="LDAP://youradpath"/>
<add key="SMSServicePW" value="yourMegaASSMSServicePassword"/>

When pressing the "**Please send OTP"** button the User ID is authenticated and if successful, an OTP is generated and SMSed to the user's Cellular phone.

Active Directory authentication and Challenge Response



This template includes sample code for Active Directory authentication and using the RequestSDResponse method.

UserID – is the Active Directory user id.
CAT Challenge – is the challenge number generated at the CAT Token
AD Password – is the Active Directory Password of the User ID.
AD Path – is the LDAP Active Directory Path. The template tries to detect the default AD Path.

When pressing the "**Get SD Response"** button the User ID is authenticated and if successful, an SD Response number is generated. This number is required for the CAT Token Add Site Manually CR menu option. When the number is entered into the CAT, the site is defined and user will see the OTP.

An Account is the virtual token the CAT manages. It is the required data for the CAT to generate an OTP on the Cellular. The Account consists of data such as:

- Web Site name
- User ID
- Secret Data
- OTP Type
- OTP Length
- Etc.

An Account can be created manually (using the CAT Menu item Add Account Manually) or it can be created and incorporated into a CAT package that is saved on the Internet under a unique name.

The action of sending the URL of the package to the user by SMS is called – **CAT Deployment**. Once the URL SMS is received the user can download the CAT by using the Cellular "Go To Web Address" option (or similar, depending on the user's cellular menu).

The CAT will immediately start to install. When the CAT is opened, the Account and OTP will be available for the user.

It is recommended that the user secures his CAT with a password and verification text.

More about easy deployment

One of the hurdles of strong authentication is the deployment of the OTP tokens to the end users. Deployment includes:

- Token delivery (and installation - in the case of soft token)
- Token activation
- Token management and maintenance

Easy deployment means – less work for the administrator, faster start for the end user and less overheads for the enterprise.

Hard tokens for example have to be purchased from the supplier, delivered to enterprise and then hand delivered to the end user, the activation has to be done by the administrator and the token device has to be purchased. Each time the token is lost or broken or the battery ends a new hard token has to be purchased.

The CAT is a soft token designed to overcome those time consuming hurdles and related costs. The delivery can be done through the Internet; it is instantaneous with no need to wait for delivery or for a purchase. We do not manage tokens – we manage Identities. The tokens are free. The end user or administrator can install any number of CAT soft tokens.

The CAT software token can be delivered to the registering users in any way the enterprise chooses: from automatic sending of the software to new registering users, to personal and secured installation of the CAT on each cellular by an administrator or support person.

The CAT Token delivery can be done by sending a download link to the cellular (or Windows OS). Sending can be done by SMS, Email or any other mean. Each cellular OS has its own CAT soft token download URL. The update URLs can be found at http://www.megaas.com

The registration of a User to a CAT protected server is usually done by the Administrator. This is the case when the enterprise is allowing access to the server only to known identities. For example, a Bank allows Bank registered clients to access their existing accounts. The Admin registers new users using the CAT Management System.

On the other hand, there are web sites that allow anonymous users to register to the web site and start using its facilities. This is an open access web site and users from all over the world can join. For example, ICQ and AMAZON are open access web sites that you are invited to register to, in order to make use of their content & services. In this case, the act of registration to the web site has to also register the user at the CAT Authentication Server for the next Login Authentication. This registration is done by request from the Enterprise Web Server using the CAT API Web Service.

Creating an Account in the CAT Token can be done manually. Using the CAT Token Menu the user is required to enter few details including:

- Web Site name – simple textual name for the user convenience
- User ID – simple textual name for the user convenience
- Secret Data – this is the Seed for creating the OTPs and synchronizing with the CAT AS. **The Secret Data has to be provided to the user prior to adding the account** manually.
- OTP Type – Mixed Characters & Numbers, Just numbers, Fixed password

CAT Token Menu option - Add Site Manually
(See the CAT Token user guide)

Providing the Secret Data to the CAT user can be done in any way the enterprise chooses to. For example, some Banks today provide Credit Cards to customers by mail. Other Banks provide the Credit Cards at the branch where the customer can be identified with credentials. Similarly the Secret Data can be sent to registered customer by SMS, Email, Mail, Special delivery etc… or it can be handed by the Administrator.

To avoid the necessity to deliver the Secret Data manually or by third party, the CAT has the Deploy Selected Identities service.

Using the Deploy Selected Identities option the administrator sends an SMS to a group of selected identities. The SMS contains a personal URL link for each identity. The URL is pointing to a predefined CAT location that contains all the Account details.

When the user downloads the URL, he can immediately start working.

More about Send OTP (SMS, Email,….)

To use the CAT AS with a sent OTP you need to:

- Configure the CAT AS to send OTP on request.
- Set identities to receive an OTP.

To configure the CAT AS to send OTP you have to configure the delivery method first by enabling and configuring one of the following:

- Configure Using SMS – Enabling delivery of SMS messages. The option is different to the next 2 options. SMS delivery requires setting an SMS provider API. This API may require any of the next 2 options.
- Configure Using Emails – Enabling delivefry of Email messages.
- Configure Using ASP – Enable using Active Pages to process an API script.

Once the delivery is enabled and set you can Configure Sending OTP.

A CAT Identity can be configured to one of the following Authentication methods:

- One Time Password (OTP). A password that changes every minute and cannot be used again once it was used. This is the default.
- Fixed Password. A password that does not change.
- **Sent OTP**. A Fixed password that is delivered to the user by external means such as SMS or Email. The Sent OTP is valid for a predefined number of minutes from the time it was sent and cannot be used again once it was used.

Identities that are set to “Sent OTP” will be authenticated by a two staged process. First, an OTP has to be sent and a time stamp is saved, than, the OTP has to be entered and it will be checked for expiration and validity.

OTP can be sent by the Send OTP Web Service or by the CAT Radius.

When using the Send OTP of the CAT API Web Service the service has to be installed and enabled. The request for sending the OTP is generated by the Enterprise Web Service after the user has been authenticated by another method such as a Fixed Password.
The OTP is usually used as a second authentication factor.

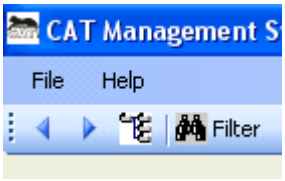
To use the CAT Radius with a send OTP you have to Configure Additional Password for the first step. For example, set the additional password to be the identity's Active Directory password. You also have to set your Login procedure to a Radius Challenge respond after entering the Active Directory.
The CAT Radius is first passed the identity id and active directory password. After authenticating the details the CAT Radius send the OTP to the identity and will respond with a Radius Challenge and wait for the next authentication request from the same identity to include the sent OTP.

Chapter 5 – Additional Tasks

The CAT MS Tools bar

The CAT Tools bar provides fast access to general options and to specific forms option.

The base option from left to right:



- Move up the Application Tree
- Move down the Application Tree
- Open the Application Tree to show all tasks
- The Data Filter is a specific option described in the following section. It is available only for certain Application Tree tasks.

All tools bar option will show a yellow tool tip when pointed at with enhanced explanation of the tool task purpose.

Using the Data Filter

The Data Filter is a Selection GUI that is available as a Toolbar option for the following Application Tree tasks:

- Identity Management tasks – available on the tools bar
- Event Viewer tasks – available on the tools bar
- Report formats – opens automatically on selection of the report format

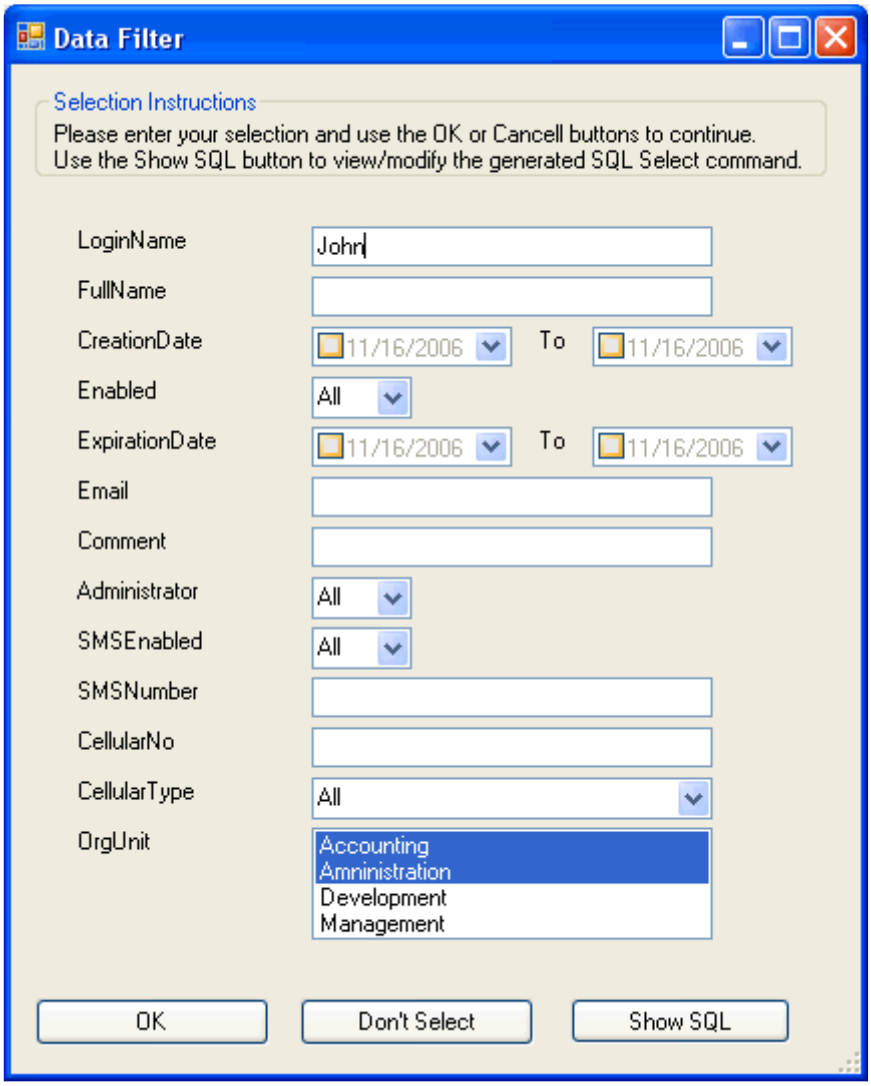
The Data Filter opens with predefined list of selection fields.

The selection fields can be categorized as:

- Numeric fields – allow you select and exact number or a rage of numbers
- Character fields – allow you to select any substring
- Dates – allow you to select an exact date or a range of dates

- Character field with a list of values – allows you to select multiple values
- Field with a drop down list – allows you to select a value from the list

For example:



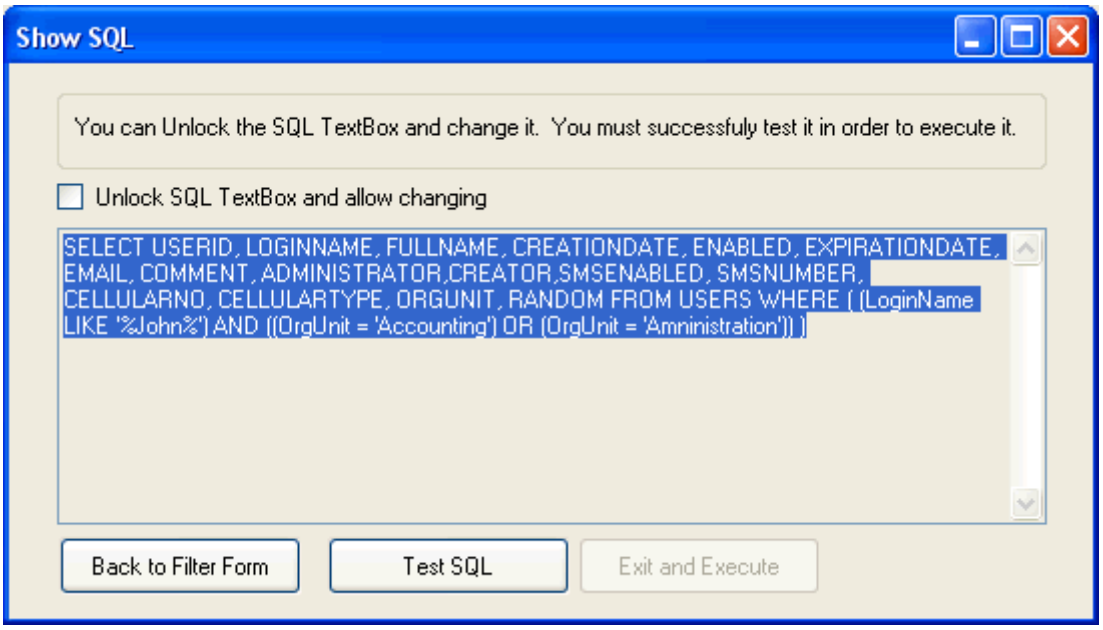
Pressing the OK will execute the selection of – All Login Names that contain John in the Organization Units of – Accounting and Administration.

The value “All” in the fields Enabled, Administrator, SMS Enabled and Cellular Type indicates that they were not used in this selection.

The dates Creation Date and Expiration Date were not used either. To use a date, you have to check the date.

Advanced SQL Statements

The Filter GUI covers most of the data selection requirements, but for those who need more advanced SQL selections there is the Show SQL option.



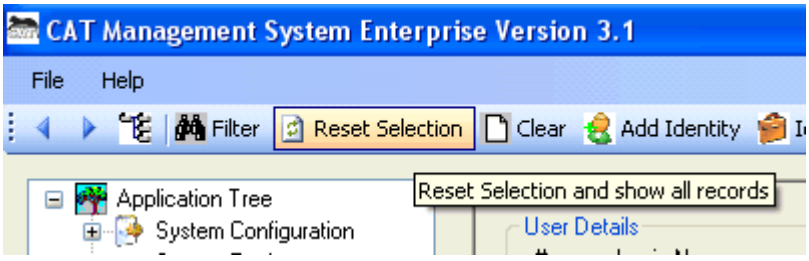
The above Show SQL is the translation of the previous Data Filter into an SQL statement. If you know SQL, you can modify the statement.

To enable modification of the SQL check the “Unlock SQL TextBox”.
Once you are done with the changes to the SQL Statement – you must Test the new SQL statement.

If the tested is successful you can “Exit and Execute” the modified SQL Statement.

Resetting the Data Filter selection

To reset the current selection in any of the data forms use the reset selection Tools bar option.



Using legacy Server Databases

The CAT MS supports 3 types of databases:

- MS Access for small installations. The CATDB.mdb file is provided with the CAT MS to be used for demonstration only.
- MS SQL Server
- MySQL

The CATDB.mdb comes with all the required tables and queries.
When the administrator selected to use MS SQL Server or MySQL, the CATDB database space has to be built in those databases prior to performing
Initiation – Step 2 .

There are two ways to build the CATDB database into another legacy database.

- *Use a database converter* and import the CATDM.mdb into the legacy database (MySQL, MS SQL Server).
- *Use the provided SQL Scripts* that can be found in the SQL Scripts sub folder of the installation folder. **Notice – the provided scripts may have to be customized to your particular DB version. Some knowledge of SQL is required.**

When importing the CATDB.mdb, make sure that all the Indexes and queries have been imported correctly and that all tables except the "EventTypes" table are empty.
Check the fields' lengths and types that they match the MS Access definitions.

Building MySQL DB

Open MySQL Administrator tool and run the "MySQLCATDB.sql" SQL Script found in the SQL Scripts folder. This will create the "catdb" database and required tables.

Use the "catdb" database in the DSN you define.

Building MS SQL Server

Open the MS SQL Server Management Studio and run the "MSSQLServer.sql" SQL Script found in the SQL Scripts folder. This will create the "CATServer" database and required tables.

Use the "CATServer" database in the DSN you define.

DSN

In the case of CAT AS installation with CAT Web Services, you need to define an additional DSN named *CATAPIServices* to the CAT database.

Chapter 6 – The Cellular Authentication Token

How does it work

The Cellular Authentication Token – CAT is a software token. The CAT has several versions for different OS and devices. The most common environment is Cellular device that can run Android or iOS.

You can find lists of supported devices in the Mega AS Ltd web site.

The CAT is stand-alone and does not require special features or active communication. It does not use SMS and has no hidden expenses.

Once the user has installed the CAT and setup the site details the user can view the site OTP. Based on an internal algorithm, the CAT shows a new One Time Password (OTP) every 60 seconds.

Installing the CAT on a Cellular

At Mega AS Ltd web site you can find detailed and updated information about the CAT installation and CAT soft tokens range.

Each Cellular device has a way to install local applications and/or games. The CAT is installed like any other cellular game on the supported device. If you don't know how to install a game on your device please contact your Cellular services provider or consult with Mega AS Support Team.

The current URL for installing on an Android device is:
www.megaas.com/downloads/catandv2.jad

The CAT has a local data store where it keeps and manages encrypted information.
A site is a remote Server that you have a User Id to Login to.

When you start using the CAT, you have to add a new site using the Menu. That will be the site you want to login to using the One Time Password generated by the CAT.

There are two options:

Add Site Manually

When you ”Add New Site Manually” you are requested to enter the following information:

- Site Name – A short string that will be the site name. For example: MegaAS for the Mega AS Consulting Ltd site or HSBC for HSBC Bank etc.
- User Id: - is your User Id at this particular site.
- Secret Data – a short string that you're getting from the Site administrator. The Secret Data is a unique identifier sometimes referred to as Seed. This identifier is a unique personal string per Identity per Site. It is different for the same identity in different sites. The Secret Data is produced by the CAT MS at the Server and has to be delivered to the user. Refer to Deploying the CAT.
- OTP (default) or Fixed password – you can use the CAT to store all your Fixed passwords as well as generate OTPs for the sits using the CAT Authentication Server. When you define a new site you can choose the password type by checking the OTP or Fixed. As default – the OTP is checked.

Quick Add Site Paste string

This option requires the administrator to send you (by SMS or Email) your unique **paste string**. The string contains all the site information including the Secret Data. For additional security, the Secret Data can be encrypted in which case the administrator will have to give you a **Password** to enter. Press **Continue** and the site is added.

After saving, the new site it automatically becomes the defaults site.
From now on each time you open the CAT this site will be on the screen with the OTP showing.

You can manage any number of sites under the same CAT.
Once you have multiple sites defined, the last one selected becomes the default site.

Notice – at any one time, there may be differences between the different CAT soft tokens for the different cellular OSs.

Deploying the CAT

CAT Deployment is providing the items that the end user needs:

- The CAT software. The user has to install the CAT software on one or more of the supported environments and devices.
- Delivering to the user its Secret Data for your site.

Both items require consideration and to be in accordance with the organization security policy.

Do not hesitate to consult with your local CAT distributor or Mega AS Consulting Ltd support team.

Also see more about easy deployment (Chapter 5)

The CAT Software

The CAT software can be downloaded from a number of sites by the end user to the device. Each organization can consider getting permission from Mega AS Consulting Ltd to provide the software from their server.

Alternatively the organization can:

- Have the CAT preinstalled on all employees (CAT users) Cellulars by the business cellular service provider.
- Send a one-time SMS message or Email to the users Cellulars. The message containing the CAT download URL can help the users to do a fast download from a secured source.
- Have the Administrator summon the end users and help them to install the CAT.

The Secret Data

Similarly, the following options can be considered for delivery of the Secret Data to a user:

- Sending a onetime SMS or Email to the user with the Secret Data upon registration. The Secret Data can be delivered encrypted for additional security.
- Mailing the Secret Data to the user in a similar way to a Credit Card PIN mailing
- Hand delivery of the Secret Data by the administrator

Appendix

New in CAT AS Version 4.1.0

- **Chapter 4 – CAT Web Services**
- Installing the CAT Web Services (Optional)
- Customize Web Services
- Customize SMS Services
- Add/Change Identity Details
- Deployed Identities' Details
- Events Management

New in CAT AS Version 4.2.0

- A New Support package for the help desk

New in CAT AS Version 4.3.0

- Active Directory Password verification option
- Support for AD Groups CATAdministrators and CATSupport
- Support for OATH TOTP authentication algorithm for Numeric OTP

New in CAT AS Version 4.4.0

- New Active Directory advanced filter option with AD Tree and support for embedded groups
- Change in behavior when displaying the Identity OTP and Secret Data
- Controlling OTP Length
- A new Secret Data challenge response setting option
- New Template for Active Directory authentication and SMS OTP sending
- New Support for a new Mega AS Ltd SMS service provider.

New in CAT AS Version 4.5.0

- The main feature of 4.5.0 is a rewrite of the CAT Web Services for performance and simplicity.
- Full support for SMS deployment and SMS OTP sending through external SMS provider in addition to the current available option of using Mega AS SMS provider.
- New Email deployment service for Email deployment end users.
- Support of the new CAT mini Radius Server. This will be the future default Radius.
- Support for FreeRadius 1.1.7 for windows
- Clear fields option for Add/Change Identities option.
- No need for SMS License Key. The SMS module is fully integrated with the CAT AS.
- Simplified DSN selection. The DB type is automatically detected.
- Additional templates for the CAT deployment by SMS.
- Updated SQL Scripts for MS SQL Server and MySQL databases.
- Internal performance issues and bug fixing.

New in CAT AS Version 4.6.0

- The main feature of 4.6.0 the new CAT mini Radius Server replacing the usage of FreeRadius. The CAT mini Radius is Windows .Net based application that supports Windows Server 20XX, Vista, XP, 7.
- Changing

New in CAT AS Version 4.8.x

- The main feature of 4.8.is the extended support for sending OTP by SMS or Email. We have also added new features for easy deployment of the CAT soft token. These new features are supported by our new CAT soft tokens.
- Additional settings and more control for the administrator.
- Improved performance.
- Few fixes to known issues

The CAT MS License Agreement

Important - Read Carefully:

This End User License Agreement (“Software License Agreement”) is a legal document between you and Mega AS Consulting Ltd. (MASC). It is important that you read this document before using the CAT software (“Software”) and any accompanying documentation , including, without limitation printed materials, ‘online’ files, or electronic documentation (“Documentation”). By clicking the “I agree” and “Next” buttons below, or by installing, or otherwise using the Software, you agree to be bound by the terms of this Software License Agreement as well as the MASC Privacy Policy (“Privacy Policy”) including, without limitation, the warranty disclaimers, limitation of liability, data use and termination provisions below, whether or not you decide to purchase the Software. You agree that this agreement is enforceable like any written agreement negotiated and signed by you. If you do not agree, you are not licensed to use the Software, and you must destroy any copies of the Software in your possession or control.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS LICENSE, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

I. GRANT

Subject to the provisions contained herein, MASC hereby grants you, Licensee a non-exclusive, non-transferable limited license to install and use one (1) copy of its proprietary software ("Software”), described as CAT and eAuthentication Service. Licensee may make one (1) copy of the SOFTWARE solely for backup or archival purposes, provided that Licensee reproduces and includes all copyright and other proprietary notice(s) on the copy.

II. DISTRIBUTION

Licensee may not distribute the SOFTWARE.

III. RESTRICTIONS

Licensee may not:

(a) Decompile, reverse engineer, disassemble or otherwise reduce the SOFTWARE to a human perceivable form.

(b) Rent, lease, lend, transfer or otherwise transfer rights to the SOFTWARE.

(c) Translate, adapt, modify the SOFTWARE or create derivative works based upon the SOFTWARE or any part thereof.

(d) Remove any proprietary notices or labels on the SOFTWARE.

(e) Use the SOFTWARE to encode, reproduce or copy any material or intellectual property you do not have the right to encode, reproduce or copy. The content recording and playback

features of this SOFTWARE are intended only for use with public domain or properly licensed content and content creation tools.

IV. TITLE

Ownership rights, and intellectual property rights in and to the Software and Documentation shall remain in MASC and/or its suppliers. This Agreement does not include the right to copy or sub-license the Software and is personal to you and therefore may not be assigned (by operation of law or otherwise) or transferred without the prior written consent of MASC. The foregoing License Agreement gives Licensee limited rights to use the SOFTWARE. You further agree not to modify or create derivative works of the Software.

V. DISCLAIMER OF WARRANTIES

THE SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, WITHOUT ARRANTY OF ANY KIND ,INCLUDING WITHOUT LIMITATION THE WARRANTIES THAT IT IS FREE OF DEFECTS, MERCHANTABLE ,FIT FOR A PARTICULAR PURPOSE, OR NONINFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE IS BORNE BY LICENSEE.SHOULD THE SOFTWARE PROVE DEFECTIVE IN ANY RESPECT, LICENSEE AND NOT LICENSOR OR ITS SUPPLIERS OR RESELLERS ASSUMES THE ENTIRE COST OF ANY SERVICE AND REPAIR. IN ADDITION, THE SECURITY MECHANISMS IMPLEMENTED BY THE SOFTWARE HAVE INHERENT LIMITATIONS, AND LICENSEE MUST DETERMINE THAT THE SOFTWARE SUFFICIENTLY MEETS ITS REQUIREMENTS.

VI. LIMITATION OF LIABILITY

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, TORT, CONTRACT, OR OTHERWISE, SHALL MASC OR ITS SUPPLIERS OR RESELLERS BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR
LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION,OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES. IN NO EVENT WILL MASC BE LIABLE FOR ANY DAMAGES IN EXCESS OF MASC'S LIST PRICE FOR A LICENSE TO THE SOFTWARE, EVEN IF MASC SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE ,SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU.

VII. ENTIRE AGREEMENT

This License Agreement constitutes the entire agreement between Licensee and MASC and supersedes any other prior agreements or understandings, whether oral or written, regarding the SOFTWARE. If a provision of this agreement is deemed null and void ,invalid or without effect, the remainder of this agreement shall remain in effect.

VIII. GOVERNING LAW

This license agreement is governed and construed in accordance with New Zealand law. You agree that any dispute shall be submitted to the jurisdiction of
Auckland, New Zealand.

Index