Opendiem Training

Exercise 14

Opendiem-TRN-0014

Revision	5.0.0		
Status	Initials	Date	Comment
Released	RAC	11/18/2010	Updated format and content

Exercise 14 – Opendiem Security

Introduction

Opendiem incorporates powerful and flexible security features, all transactions to/from the Server are subject to security procedures that ensure the data on the system is protected from unauthorized access.

- Secure User Authentication employing 128-bit industry standard MD5 digital signatures.
- Data may be set to Read Only, Read/Write (full access) or no access. This feature allows the security administrator to permit different users to access different features of the system. For example a user with no access rights to Card Access system related information would see no graphics or data on pages containing this information whereas a user with full access rights would be able to view this information and make changes to it.
- Security is based on users and groups; each user has an individual profile (user name, logon id, password etc.) and may belong to one or more groups. Each group is then granted access to data items in the system as required.
- Access may be granted at any level on the data hierarchy, at an individual data item level or node level (or pre-defined group of data items).

Objective

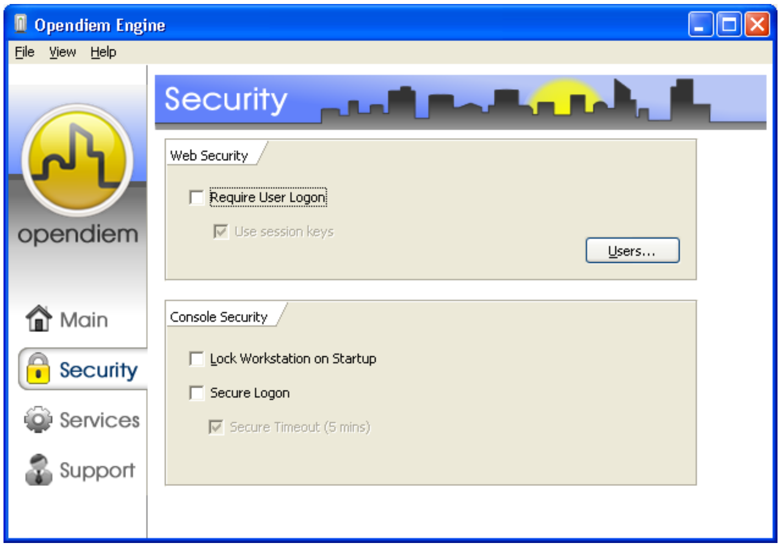
In this exercise you will investigate Opendiem security features, you will set up users and groups and setup security privileges for a group. Verification of the security settings will be carried out by connecting with a Web Browser and security events will be audited using the Opendiem log. Finally you will learn how to change user passwords via a Web Browser.

Re-opening the project in Opendiem Designer

Exercise Instructions

Ensure that Opendiem Engine is running on your Server and if necessary restart it. If Opendiem Designer is running, close it down.

Select the Security page on Opendiem Engine as shown below:



Web Security

☐ Require User Logon

☑ Use session keys

Console Security

☐ Lock Workstation on Startup

☐ Secure Logon

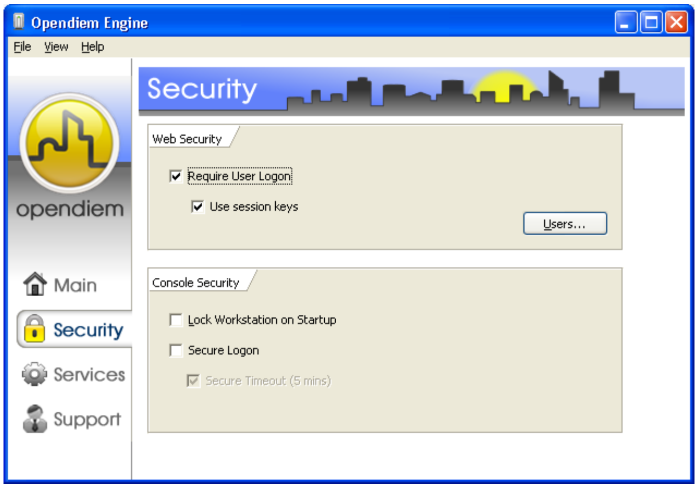
☑ Secure Timeout (5 mins)

Opendiem Security Page

Opendiem has two servers, a Web server (Microsoft IIS) which responds to http requests and serves Web pages and graphics to port 80 by default, a second server the Opendiem Server serves Opendiem Protocol data on port 4400 by default. Opendiem requires two servers as the http protocol used by most Web browsers is a stateless protocol which means that a connection is established, data is requested, delivered and then the connection is released. To provide live data updates within the Web browser the Opendiem server maintains a connection to update each of the Web Clients with the latest available data.

From a security perspective this means that security must be enabled for each server. Opendiem provides a session key facility to permit the use of one user name /password for both servers within a session, this is provided as a convenience, but can theoretically compromise security.

1. Check the security settings on Opendiem Engine as shown below, we will use Session Keys as a convenience to the user.



Security

Web Security

☑ Require User Logon

☑ Use session keys

Console Security

□ Lock Workstation on Startup

□ Secure Logon

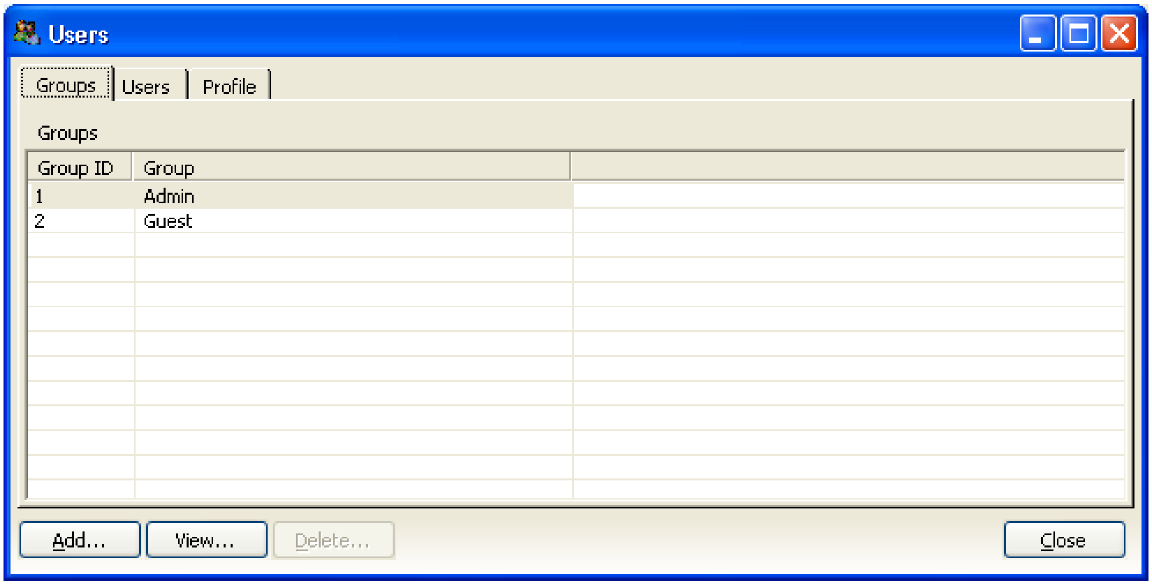
☑ Secure Timeout (5 mins)

Enabling Security

2. Click on the **Users...** button and the screen below will show.

3. To add a new security group, right click on the Group panel as shown and select **Add Group...**

4. Enter a group name such as `‘training’` into the pop-up dialog.

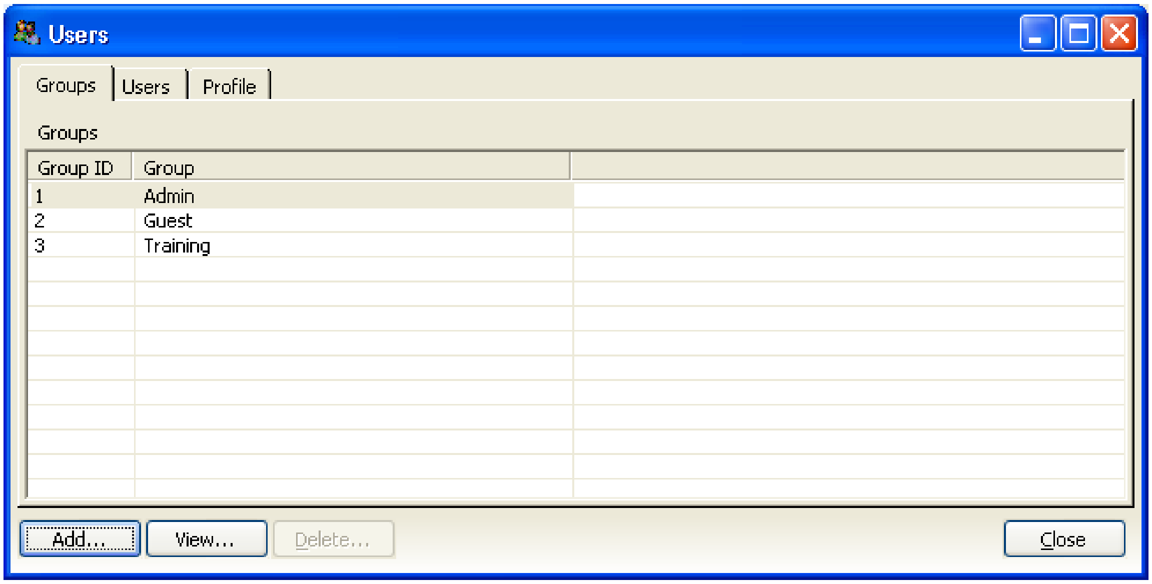


Groups

Group ID	Group
1	Admin
2	Guest

Adding security Groups

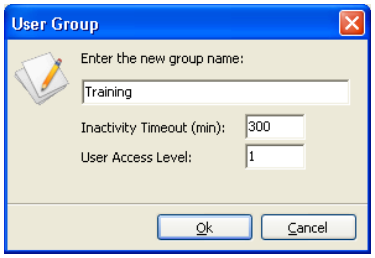
5. The new group will be added to the list of groups as shown.



Group ID	Group
1	Admin
2	Guest
3	Training

Groups listing

Select a group and then click on **Edit.. ,** the **User Group** dialogue below will show:



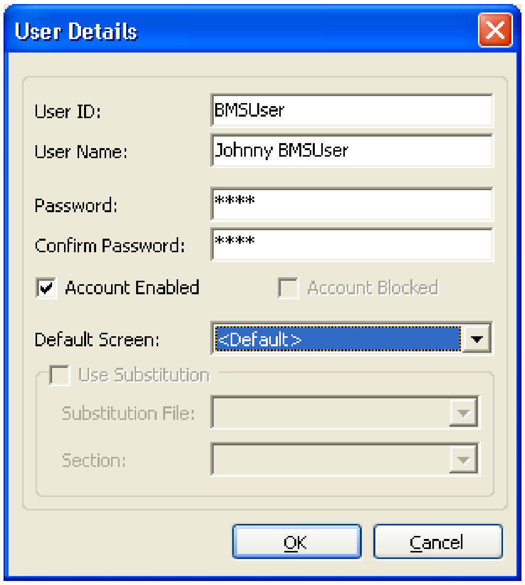
Enter the new group name: Training

Inactivity Timeout (min): 300

User Access Level: 1

This dialogue allows you to specify an Inactivity Timeout for the group. When a user who is a member of the specified group is connected via a Web Browser they will be automatically disconnected after a period of inactivity specified above. If the value is set to 0 then the inactivity timeout is disabled for that group. If a user is a member of more than one group then the highest inactivity timeout value available will be used.

6. Next, click on the **Users** tab and click right to add a new user. Enter the new user details as shown below.



User ID: BMSUser

User Name: Johnny BMSUser

Password: ****

Confirm Password: ****

☑ Account Enabled ☐ Account Blocked

Default Screen: <Default>

☐ Use Substitution

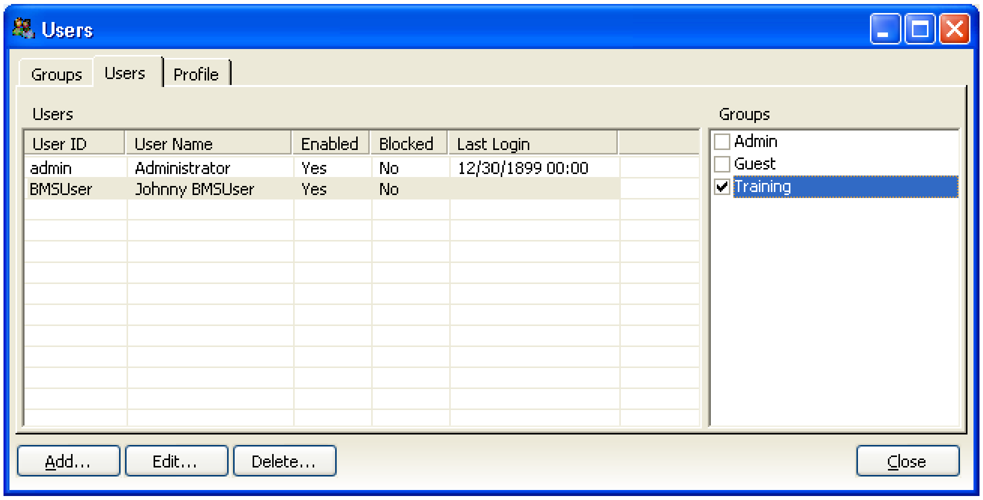
Substitution File:

Section:

Adding a new user

7. The **Default Screen:** and **Use Substitution** settings above can be used load the selected Opendiem Screen (and substitution settings if used) for an individual user whenever they log on. For this exercise we will leave these settings at the default and leave the additional settings for you to investigate at a later time.

8. Next, associate a user with one or more groups by clicking in the **Groups** checkboxes as shown below.



Users

User ID	User Name	Enabled	Blocked	Last Login
admin	Administrator	Yes	No	12/30/1899 00:00
BMSUser	Johnny BMSUser	Yes	No	

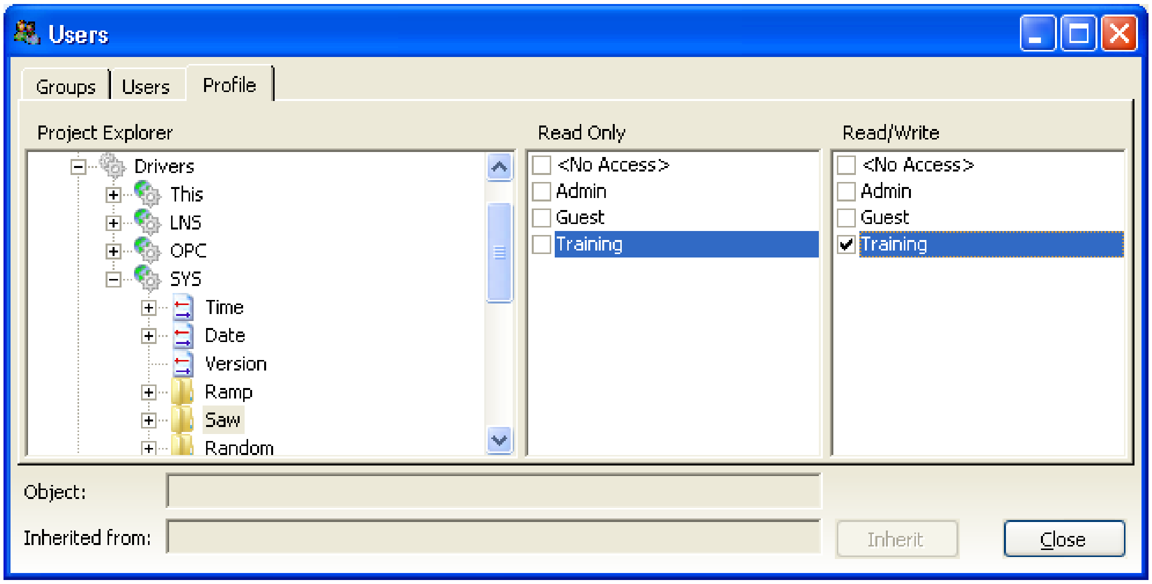
Groups

☐ Admin
☐ Guest
☑ Training

Adding Users to Groups

9. Click on the **Profile** tab. The screen below will appear, from here we will select the security profile for a group. Expand the **Project Explorer** view as shown. Security settings are hierarchical and can be applied at any level in tree. When checking for a security setting to apply Opendiem starts at the lowest level in the tree and works it's way up until it finds a security setting to apply. Using this method it is possible to set security for a complete driver or subsystem very quickly and to refine the security settings by expanding the hierarchy. Note that it is possible to apply security to screens, however it is more often than not the data that must be secured and this is carried out at the Driver level.

10. For this exercise we will apply security settings to the **SYS** driver to allow access to different data items.



Read Only

☐ <No Access>
☐ Admin
☐ Guest
☐ Training

Read/Write

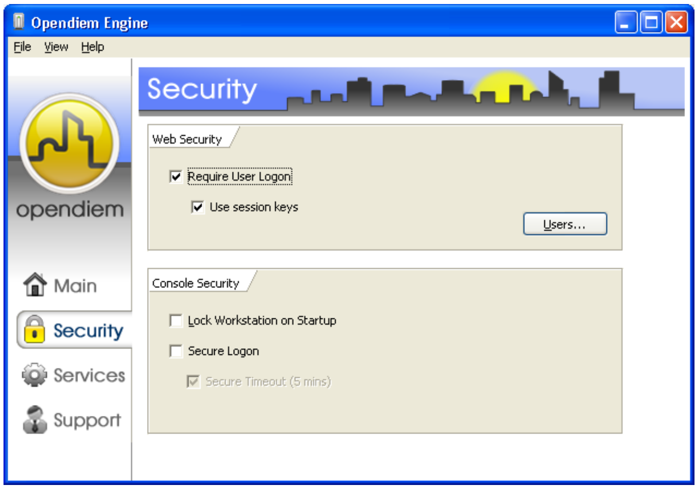
☐ <No Access>
☐ Admin
☐ Guest
☑ Training

Setting the security profile for a group.

11. Expand the tree to show the **Sys** driver **Text** register as shown below. To illustrate the different security settings set the **Text.1** to **Read Only** and **Text.2** to **Read/Write** for group **training**.

With Security Enabled

Again, Security is enabled when the Require User Logon box is checked**.**



Web Security

☑ Require User Logon

☑ Use session keys

Users...

Console Security

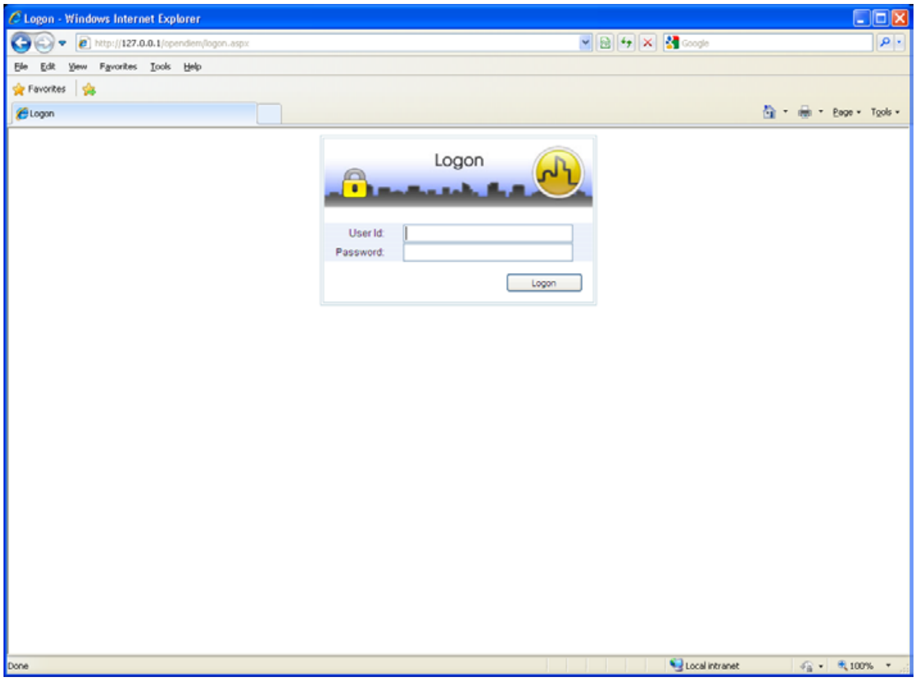
□ Lock Workstation on Startup

□ Secure Logon

☑ Secure Timeout (5 mins)

Security and Viewing Opendiem Screens

Start a browser connection, you will be prompted for a user name and password as shown below, enter the details you set earlier and click **OK**.


Logon - Windows Internet Explorer
http://127.0.0.1/opendiem/logon.aspx
File Edit View Favorites Tools Help
Favorites
Logon
Page Tools
Logon
Done
Local intranet
100%

User Id:

Password:

Logon

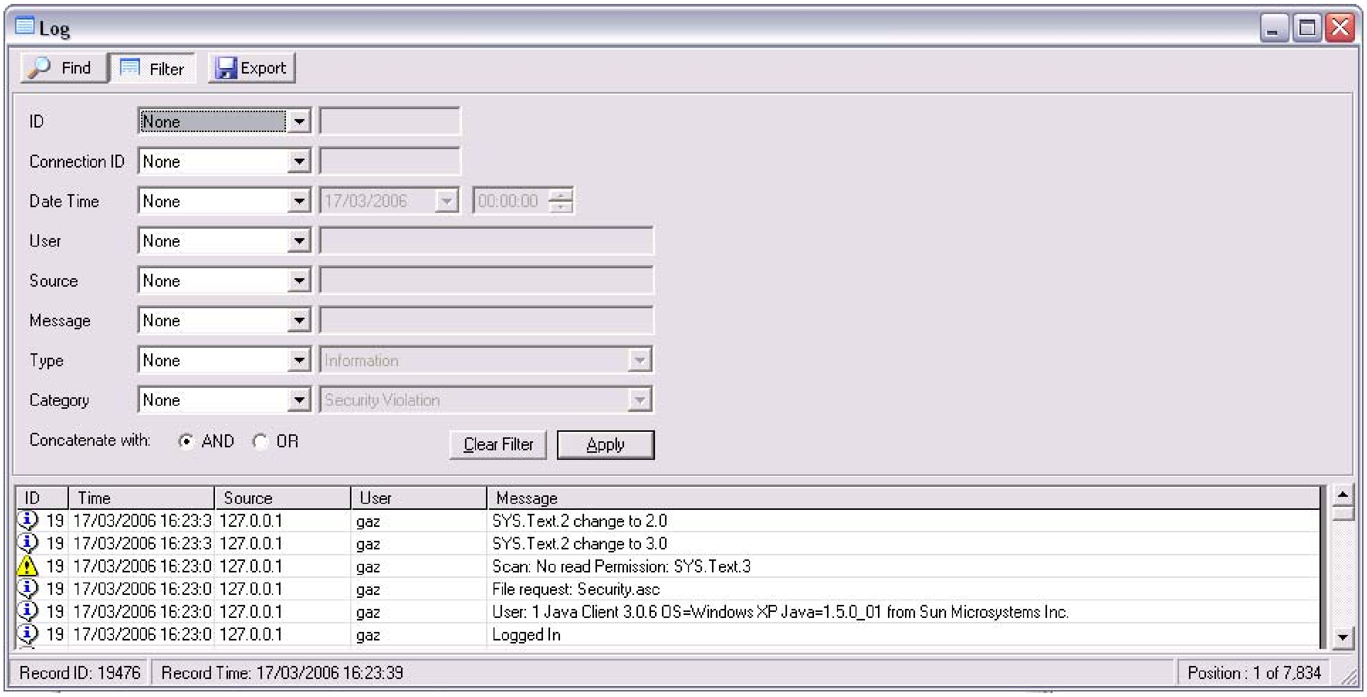
User Name and Password prompt

Once the user name and password have been successfully entered the browser will connect to the pre-defined Opendiem start screen for that user (as defined in their User profile). If data appears as *** the items are blocked due to security settings. The data display as *** to distinguish them from items that cannot be displayed for other reasons such as network failures which are displayed as ???.

Opendiem Audit Log

The Audit Log details all system activity including date/time of event, IP address of the client involved and the user name (if logged on) along with the event description text.

The Audit log has several features that make diagnosing problems easier, a find function allows the log to be searched for any text string. The filter function allows standard filtering options to be applied to the log to display only the items of interest, in the screen below a filter has been applied to show only the items containing 'no write'.



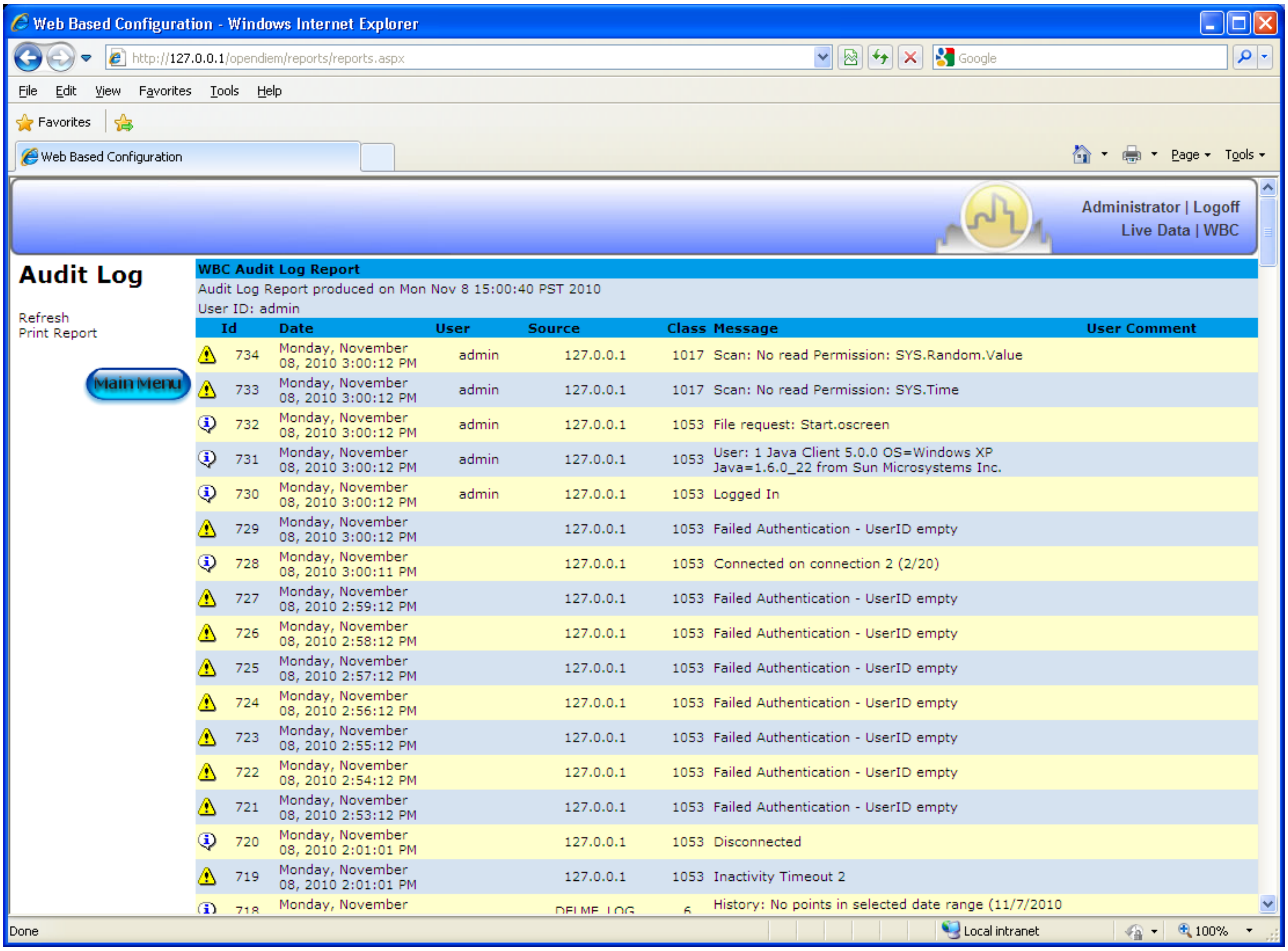
ID: None
Connection ID: None
Date Time: None 17/03/2006 00:00:00
User: None
Source: None
Message: None
Type: None Information
Category: None Security Violation
Concatenate with: ● AND ○ OR

ID	Time	Source	User	Message
ⓘ 19	17/03/2006 16:23:3	127.0.0.1	gaz	SYS.Text.2 change to 2.0
ⓘ 19	17/03/2006 16:23:3	127.0.0.1	gaz	SYS.Text.2 change to 3.0
⚠ 19	17/03/2006 16:23:0	127.0.0.1	gaz	Scan: No read Permission: SYS.Text.3
ⓘ 19	17/03/2006 16:23:0	127.0.0.1	gaz	File request: Security.asc
ⓘ 19	17/03/2006 16:23:0	127.0.0.1	gaz	User: 1 Java Client 3.0.6 OS=Windows XP Java=1.5.0_01 from Sun Microsystems Inc.
ⓘ 19	17/03/2006 16:23:0	127.0.0.1	gaz	Logged In

Record ID: 19476 Record Time: 17/03/2006 16:23:39 Position : 1 of 7,834

The audit log is also available via a Web browser, enter the server IP address followed by '`Opendiem/reports/reports.aspx`'. Start a browser and enter '`http://localhost/Opendiem/reports/reports.aspx`' into the address bar.

A screen containing the audit log will appear as shown below:



Audit Log

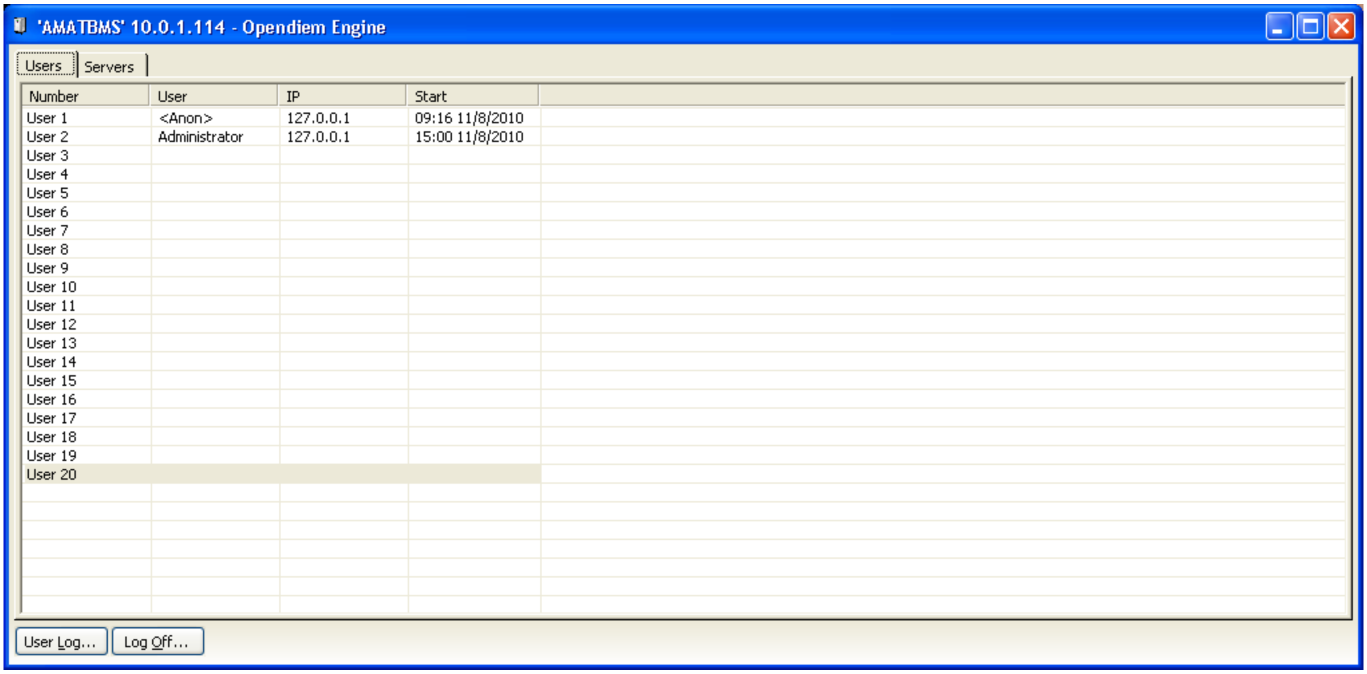
WBC Audit Log Report

Audit Log Report produced on Mon Nov 8 15:00:40 PST 2010

User ID: admin

	Id	Date	User	Source	Class	Message	User Comment
⚠	734	Monday, November 08, 2010 3:00:12 PM	admin	127.0.0.1	1017	Scan: No read Permission: SYS.Random.Value	
⚠	733	Monday, November 08, 2010 3:00:12 PM	admin	127.0.0.1	1017	Scan: No read Permission: SYS.Time	
ⓘ	732	Monday, November 08, 2010 3:00:12 PM	admin	127.0.0.1	1053	File request: Start.oscreen	
ⓘ	731	Monday, November 08, 2010 3:00:12 PM	admin	127.0.0.1	1053	User: 1 Java Client 5.0.0 OS=Windows XP Java=1.6.0_22 from Sun Microsystems Inc.	
ⓘ	730	Monday, November 08, 2010 3:00:12 PM	admin	127.0.0.1	1053	Logged In	
⚠	729	Monday, November 08, 2010 3:00:12 PM		127.0.0.1	1053	Failed Authentication - UserID empty	
ⓘ	728	Monday, November 08, 2010 3:00:11 PM		127.0.0.1	1053	Connected on connection 2 (2/20)	
⚠	727	Monday, November 08, 2010 2:59:12 PM		127.0.0.1	1053	Failed Authentication - UserID empty	
⚠	726	Monday, November 08, 2010 2:58:12 PM		127.0.0.1	1053	Failed Authentication - UserID empty	
⚠	725	Monday, November 08, 2010 2:57:12 PM		127.0.0.1	1053	Failed Authentication - UserID empty	
⚠	724	Monday, November 08, 2010 2:56:12 PM		127.0.0.1	1053	Failed Authentication - UserID empty	
⚠	723	Monday, November 08, 2010 2:55:12 PM		127.0.0.1	1053	Failed Authentication - UserID empty	
⚠	722	Monday, November 08, 2010 2:54:12 PM		127.0.0.1	1053	Failed Authentication - UserID empty	
⚠	721	Monday, November 08, 2010 2:53:12 PM		127.0.0.1	1053	Failed Authentication - UserID empty	
ⓘ	720	Monday, November 08, 2010 2:01:01 PM		127.0.0.1	1053	Disconnected	
⚠	719	Monday, November 08, 2010 2:01:01 PM		127.0.0.1	1053	Inactivity Timeout 2	
ⓘ	718	Monday, November		DELME_LOG	6	History: No points in selected date range (11/7/2010	

When a user logs on to Opendiem, information for the user is available from the Opendiem Server. Open the Opendiem Server service and click on the **Users** tab as shown below. The screen shows the user name, IP address and start time and date of the current log on session.

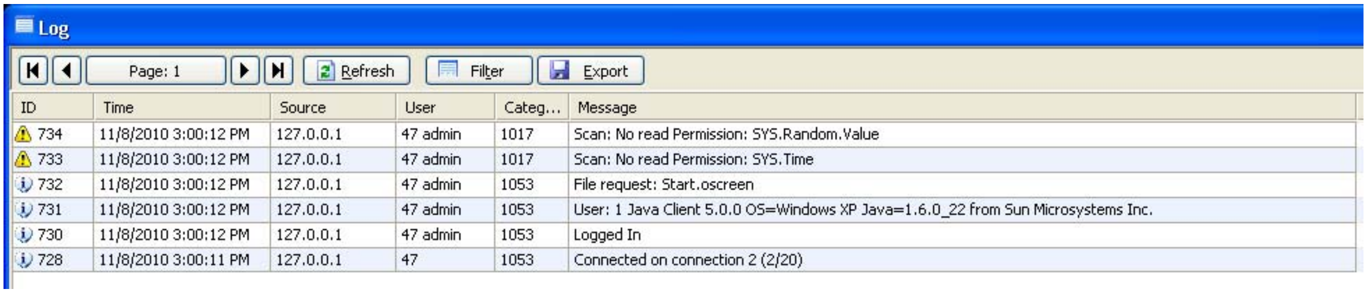


'AMATBMS' 10.0.1.114 - Opendiem Engine

Number	User	IP	Start
User 1	<Anon>	127.0.0.1	09:16 11/8/2010
User 2	Administrator	127.0.0.1	15:00 11/8/2010
User 3			
User 4			
User 5			
User 6			
User 7			
User 8			
User 9			
User 10			
User 11			
User 12			
User 13			
User 14			
User 15			
User 16			
User 17			
User 18			
User 19			
User 20			

Opendiem Server screen

Click on **User Log…** and an audit log for the selected user will be appear as shown below. The User Log has the same search and filter capabilities as the audit log.

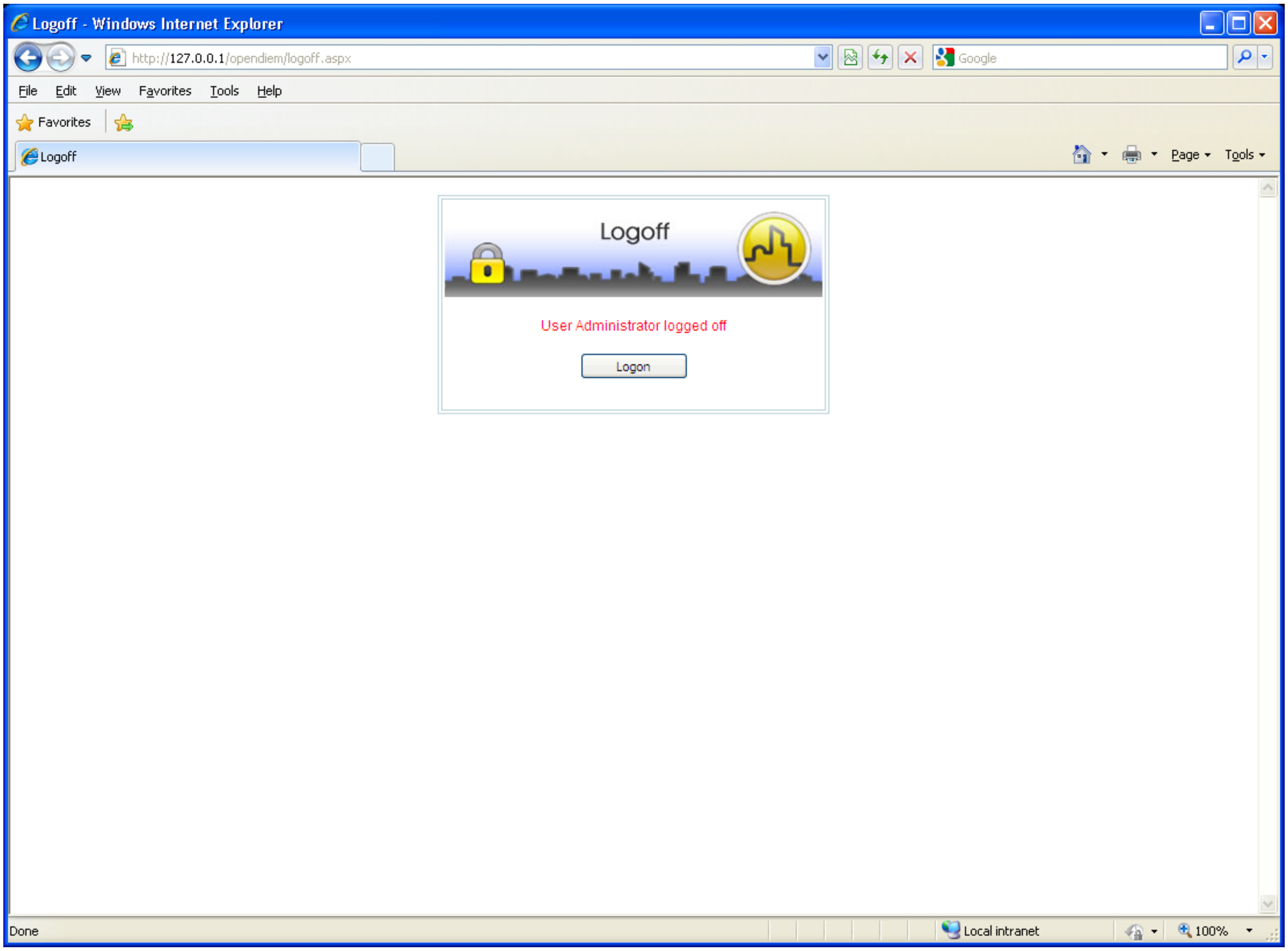


Log

ID	Time	Source	User	Categ...	Message
⚠ 734	11/8/2010 3:00:12 PM	127.0.0.1	47 admin	1017	Scan: No read Permission: SYS.Random.Value
⚠ 733	11/8/2010 3:00:12 PM	127.0.0.1	47 admin	1017	Scan: No read Permission: SYS.Time
ℹ 732	11/8/2010 3:00:12 PM	127.0.0.1	47 admin	1053	File request: Start.oscreen
ℹ 731	11/8/2010 3:00:12 PM	127.0.0.1	47 admin	1053	User: 1 Java Client 5.0.0 OS=Windows XP Java=1.6.0_22 from Sun Microsystems Inc.
ℹ 730	11/8/2010 3:00:12 PM	127.0.0.1	47 admin	1053	Logged In
ℹ 728	11/8/2010 3:00:11 PM	127.0.0.1	47	1053	Connected on connection 2 (2/20)

User Audit log

Force a user log off by selecting the user and clicking on **Log Off…** Confirm your action and the user will be logged off the system and the client browser will display a message as shown below.



Logoff - Windows Internet Explorer
http://127.0.0.1/opendiem/logoff.aspx
Google
File Edit View Favorites Tools Help
Favorites
Logoff
Page Tools
Logoff
Logon
Done
Local intranet
100%

User Administrator logged off

Additional Information

Web Server security mechanisms explained:

Basic Access Authentication

The basic authentication scheme assumes that your (the client's) credentials consist of a username and a password where the latter is a secret known only to you and the server.
The server's 401 response contains an authentication challenge consisting of the token "Basic" and a name-value pair specifying the name of the protected realm. Example:
WWW-Authenticate: Basic realm="Control Panel"

Upon receipt of the server's 401 response, your web browser prompts you for the username and password associated with that realm. The Authentication header of your browser's follow-up request again contains the token "Basic" and the base64-encoded concatenation of the username, a colon, and the password.
Authorization: Basic QWRtaW46Zm9vYmFy

The server base64-decodes the credentials and compares them against his username-password database. If it finds a match, you are in.
The major drawback of the basic authentication scheme is that it is relatively simple for eavesdroppers to spy out your password since it is transmitted in plain sight.

Using of Cryptography

An alternative authentication scheme known as digest authentication remedies this weakness through the use of cryptographic hashes, usually the MD5 message digest algorithm.
MD5 as used by Opendiem takes an input string of arbitrary length and computes a 128-bit number from it, i.e. there are 2^128 = 340,282,366,920,938,463,463,374,607,431,768,211,456 different result values. Since MD5 is a one-way function, it is virtually impossible to reverse the computation and obtain the input value from the output value.

Now, if you just took your username and password, ran them thru MD5 as you do with base64 for basic authentication and sent the result to the server, a hypothetical eavesdropper could obviously record your hashed username and password. When prompted by the server to authenticate himself, he could then simply send your hashed password to get in. This is called a replay attack.

Digest Access Authentication

To securely prevent replay attacks, a more sophisticated procedure is obviously neccessary: the digest access authentication scheme as used by Opendiem.
First, the WWW-Authenticate header of the server's initial 401 response contains a few more name-value pairs beyond the realm string, including a value called a nonce. It is the server's responsibility to make sure that every 401 response comes with a unique, previously unused nonce value.
The Authentication header of your browsers follow-up request contains your clear-text username, the nonce value it just received, and the so-called digest-request, which it might compute as follows (if it were written in UserTalk):

```
A1 = string.hashMD5 (username + ":" + realm + ":" + password)

A2 = string.hashMD5 (paramTable.method + ":" + paramTable.uri)

requestdigest = string.hashMD5 (A1 + ":" + nonce + ":" + A2)
```

Since all these input values are either known to the server or are part of the request headers, it can do the same computation you did and if its computation yields the same request digest, it can be sure that you are in possession of the correct password.
Further, since the MD5 algorithm is not reversible, hypothetical eavesdroppers can't obtain your password from the request digest. Also, the server can quite effectively prevent replay attacks by not accepting a nonce value for more than a single authentication request. For the next request, the server hands out a different nonce value, so that the client has to compute the request digest anew.

End of Exercise 14

In this exercise we configured Opendiem security to prevent unauthorized access to the system data and verified the settings by consulting the Opendiem Log. Use of the audit log was also introduced along with filtering options. The Web based Audit log was also reviewed. Finally the user logon and password were used to access the system via a standard Web browser.

Notes:

Version 5.00 November 2010

Building Clouds
3229 Whipple Road
Union City, CA 94587

Email: support@buildingclouds.com
http://www.buildingclouds.com