ATNA Test Case Document

Prepared by ViSolve
Contact: 408.666.4320
Email: vicareplus_support@visolve.com

www.vicareplus.com

18th January 2010

Table of Contents

I. OpenEMR Audit Test Cases

For the test cases below, the OpenEMR Log Viewer is accessed by the menu
`Administration -> Other -> Logs`

CCHIT Audit Test Cases

1. Verify that Patient Record Create events are audited

Login to OpenEMR, and create a new patient. Go to the Log Viewer. Check that multiple patient-record-insert events are shown. The Patient's ID number is displayed at the top of OpenEMR, like John Smith (254). Make sure the number in the Patient ID column matches the new patient's ID.

2. Verify that Patient Record View events are audited

Select another patient, then go to the Log Viewer. Check that new patient-record-select events are shown, with a Patient ID matching the patient selected.

3. Verify the User, Event Name, Event Type, and Checksum options in the Log Viewer

Populate the audit log by logging in to OpenEMR using different usernames. For each login, create a new patient, and view other patients. Then go to the Log Viewer. Verfiy that the audit entries displayed are filtered properly when you select:
* A user from the "User" drop down list
* An Event Name (login, logout, patient-record, etc)
* An Event Type (select, insert, update, etc)

4. Verify that the audit log can only be viewed with Administrators priviledges

Create a new user 'testuser' with Access Control to Accounting, Clinician, Front Office, Physician, but not Administrators. Login as 'testuser'. Verify that there are no menu options under Administration -> Other.

5. Verify that audit events can be enabled/disabled in globals.php

In globals.php, set
$GLOBALS["audit_events"]=array("patient-record"=>0, ...

Create a new patient. Verify that no audit entry is made.

II. Audit Trail and Node Authentication (ATNA) Test Cases

ATNA involves transmitting audit records to a remote machine, according to the following protocols:

- RFC 3881 - Defines XML Message format for Audit Messages
- RFC 5425 - Defines the connection protocol, syslog over TLS.

Setting up a TLS Audit Repository Server

The test cases below require the following certificates:

```
cacert.pem    - A self-signed CA certificate
cacert.key    - The private key for cacert.pem
server.pem    - A server certificate signed by cacert.pem.
                Has the subject "/C=US/CN=localhost".
server.key    - The private key for server.pem
client.pem    - Has both the client certificate and private key, signed by
                cacert.pem.  Has the subject "/C=US/CN=user@localhost"
serverbad.pem - An invalid (non-CA signed) server certificate
serverbad.key - The private key for serverbad.pem
clientbad.pem - An invalid (non-CA signed) client certificate and key.
```

Create the certificates above using the following commands:

Create the CA certificate and key

```
# openssl req -new -x509 -nodes -subj "/C=US/CN=CertificateAuthority" \
  -newkey rsa:1024 -keyout cakey.pem  -out cacert.pem
```

Create the server certificate and key

```
# openssl req -new -nodes -subj "/C=US/CN=localhost" \
  -newkey rsa:1024 -keyout server.key -out server.req
# openssl x509 -days 365 -CA cacert.pem -CAkey cakey.pem -set_serial 10 \
  -req -in server.req -out server.pem
# rm -f server.req
```

Create the client certificate and key

```
# openssl req -new -nodes -subj "/C=US/CN=user@localhost" \
  -newkey rsa:1024 -keyout client.key -out client.req
# openssl x509 -days 365 -CA cacert.pem -CAkey cakey.pem -set_serial 11 \
  -req -in client.req -out client.tmp
# cat client.tmp client.key > client.pem
# rm -f client.req client.tmp client.key
```

Create the invalid server certificate.

```
# openssl req -new -x509 -nodes -subj "/C=US/CN=badlocalhost" \
  -newkey rsa:1024 -keyout serverbad.key  -out serverbad.pem
```

Create the invalid client certificate.

```
# openssl req -new -x509 -nodes -subj "/C=US/CN=user@badlocalhost" \
  -newkey rsa:1024 -keyout clientbad.pem  -out clientbad.pem
```

1. Test that ATNA messages are received by ATNA repository server.

In globals.php, configure the ATNA settings:
$GLOBALS['atna_audit_host'] = 'localhost';
$GLOBALS['atna_audit_port'] = 6514;
$GLOBALS['atna_audit_localcert'] = '/tmp/client.pem';
$GLOBALS['atna_audit_cacert'] = '/tmp/cacert.pem';

We will use the openssl s_server as the ATNA repository server. The s_server tool simply listens for requests, and prints the received messages to the console.

Start the ATNA repository server:

```
# openssl s_server -tls1 -verify 10 -CAfile /tmp/cacert.pem \
  -key /tmp/serverkey.pem  -cert servercert.pem  -accept 6514
```

Login to OpenEMR. Verify that the output shows XML audit messages.

2. Check that OpenEMR sends a client SSL certificate

The s_server output should show the subject and issuer of the client certificate:

```
subject=/C=US/CN=user@localhost
issuer=/C=US/CN=CertificateAuthority
```

3. Check that the XML message has a syslog header (RFC 5424)

The XML Message should begin with the following:
`<13> datetime hostname <?xml ...`

For example:
`<13> 2010-01-14T19:25:15-08:00 vicare.visolve.com <?xml`

The <13> indicates that this is an audit message

4. Check that the Login XML message is received.

The first XML message shown in the s_server output should be a Login XML message.
An example is shown below. The real message will be on a single line, not multiple lines.
Check that the displayName is "Login", the NetworkAccessPointID IP addresses are correct, and that the ParticipantObjectID matches the login name. These are highlighted in blue below:

```
<13> 2010-01-14T19:25:15-08:00 vicare.visolve.com
<?xml version="1.0" encoding="ASCII"?>
<AuditMessage xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="healthcare-security-audit.xsd">
<EventIdentification
   EventActionCode="E"
   EventDateTime="2010-01-14T19:25:15-08:00"
   EventOutcomeIndicator="4">
```

```
<EventID
   code="eventIDcode"
   displayName="Login"
   codeSystemName="DCM" />
</EventIdentification>
<ActiveParticipant
   UserID="vicare.visolve.com|OpenEMR"
   UserIsRequestor="true"
   NetworkAccessPointID="76.212.18.42"
   NetworkAccessPointTypeCode="2" >
<RoleIDCode
   code="110153"
   displayName="Source"
   codeSystemName="DCM" />
</ActiveParticipant>
<ActiveParticipant
   UserID="127.0.0.1"
   UserIsRequestor="false"
   NetworkAccessPointID="127.0.0.1"
   NetworkAccessPointTypeCode="2" >
<RoleIDCode
   code="110152"
   displayName="Destination"
   codeSystemName="DCM" />
</ActiveParticipant>
<AuditSourceIdentification
  AuditSourceID="vicare.visolve.com|OpenEMR" />
<ParticipantObjectIdentification
   ParticipantObjectID="admin"
   ParticipantObjectTypeCode="1"
   ParticipantObjectTypeCodeRole="6" >
<ParticipantObjectIDTypeCode
   code="11"
   displayName="User Identifier"
   codeSystemName="RFC-3881" />
</ParticipantObjectIdentification>
</AuditMessage>
```

5. Select a patient, and check that a Patient-Record message is received

Select a patient to view. The s_server should receive multiple "Patient Record" messages. Verify that the correct patient number is included in the message (shown in blue below).

```
<13> 2010-01-15T18:25:53-08:00 vicare.visolve.com
<?xml version="1.0" encoding="ASCII"?>
<AuditMessage xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="healthcare-security-audit.xsd">
<EventIdentification
   EventActionCode="R"
   EventDateTime="2010-01-15T18:25:53-08:00"
   EventOutcomeIndicator="4">
<EventID
   code="eventIDcode"
   displayName="Patient Record"
   codeSystemName="DCM" />
</EventIdentification>
<ActiveParticipant
   UserID="vicare.visolve.com|OpenEMR"
   UserIsRequestor="true"
```

```
   NetworkAccessPointID="76.212.18.42"
   NetworkAccessPointTypeCode="2" >
<RoleIDCode
   code="110153"
   displayName="Source"
   codeSystemName="DCM" />
</ActiveParticipant>
<ActiveParticipant
   UserID="127.0.0.1"
   UserIsRequestor="false"
   NetworkAccessPointID="127.0.0.1"
   NetworkAccessPointTypeCode="2" >
<RoleIDCode
   code="110152"
   displayName="Destination"
   codeSystemName="DCM" />
</ActiveParticipant>
<AuditSourceIdentification
   AuditSourceID="vicare.visolve.com|OpenEMR" />
<ParticipantObjectIdentification
   ParticipantObjectID="admin"
   ParticipantObjectTypeCode="1"
   ParticipantObjectTypeCodeRole="6" >
<ParticipantObjectIDTypeCode
   code="11"
   displayName="User Identifier"
   codeSystemName="RFC-3881" />
</ParticipantObjectIdentification>
<ParticipantObjectIdentification
   ParticipantObjectID="23"
   ParticipantObjectTypeCode="1"
   ParticipantObjectTypeCodeRole="1" >
<ParticipantObjectIDTypeCode
   code="2"
   displayName="Patient Number"
   codeSystemName="RFC-3881" />
</ParticipantObjectIdentification>
</AuditMessage>
```

6. Test that OpenEMR continues to work if the ATNA server is down

Stop the openssl s_server, and continue to use OpenEMR. Go to the Log Viewer page, and verify that audit events are still being saved by OpenEMR to the local log table.