Access Security Gateway — Job Aid For Messaging Products

FOREWORD.................................................................................................................................2
WHAT IS ASG ..........................................................................................................................2
WHY USE ASG .......................................................................................................................2
ASG LOCK vs ASG GUARD ......................................................................................................2
CHALLENGE – WHAT THE INTUITY SENDS ...........................................................................2
RESPONSE – WHAT THE CALLER SENDS ..............................................................................3
ASG TOKEN SERVER ...............................................................................................................3
ADMINISTERING ASG IN THE INTUITY ..............................................................................3
Assigning the Alarm ID ........................................................................................................4
Enabling ASG for a Login Id ...................................................................................................4
Enabling ASG for a com port ..................................................................................................4
EXAMPLE — SUCCESSFUL LOGIN USING ASG .................................................................5
TROUBLESHOOTING ...............................................................................................................6
What Should Happen ...............................................................................................................6
The Default Product Id ..........................................................................................................6
Are You Using The Right Tool? ............................................................................................6
ASG MOBILE ..........................................................................................................................6
TSCSS/Maestro .......................................................................................................................6
“connect” tool .......................................................................................................................7
Product Alarm id matches INADS alarm id .........................................................................7
Product Alarm id does not match INADS alarm id ...............................................................7
Try Another Login Id ...........................................................................................................7
Changing The Product’s Alarm Id .......................................................................................7
Contact The INADS Database Administration Group .......................................................8
Specific Faults .......................................................................................................................8
RECOVERING ASG FROM CUSTOMER BACKUP ................................................................8
RELOADING ASG SOFTWARE ..............................................................................................8
CUSTOMER USE OF ASG .....................................................................................................8
Enabling ASG on Customer Login ids ................................................................................9
To avoid using multiple secure tokens ...............................................................................9
Using ASG Guard and ASG Lock .........................................................................................9
ASG Guard and the RMB ......................................................................................................9
ASG KEY CHANGER .............................................................................................................9
WHERE TO GET MORE INFORMATION ...........................................................................10
ASG Used With Intuity ..........................................................................................................10
ASG Operational Guidelines .............................................................................................10
FOREWORD
This document is an attempt to explain what ASG is, why customers would want it, and what we in technical support roles need to know about ASG. We need to remember that customers expect us to be knowledgeable about ASG, and know exactly what to do if ASG – for whatever reason – should prevent us from accessing the customer’s system.

Efforts have been taken to ensure that, should an ASG failure occur, Avaya is able to recover our access to the system without further disrupting the customer's service. Many ASG documents exist (there are references listed at the end of this document) which can be referenced if you require more detail; however, this ASG job aid should provide you with all the information on ASG that you will need.

Throughout this document, I refer to the Intuity AUDIX, as it’s the ASG-equipped product I’m most familiar with.

WHAT IS ASG
ASG is authentication software that resides on the customer’s product. At present, the only messaging products to utilize ASG are Intuity Release 4.4-7 and 5.X. Note: The only release 4 system to support ASG is 4.4-7; nothing earlier. The software ensures the customer that only authorized users are accessing their systems. If you remember the Remote Port Security Device (RPSD), you’re familiar with the ASG concept (in fact, the ASG software is the same software the RPSD locks used).

ASG can be programmed to protect any Intuity login id.

WHY USE ASG
Customers are increasingly concerned about the security of their LAN servers. As Avaya places devices on the customer’s LAN, we become responsible for ensuring the customer that these Avaya products are being accessed only by Avaya employees, and only for authorized purposes such as resolving maintenance issues.

ASG LOCK vs ASG GUARD
ASG protection is provided in two different forms:
- ASG Lock. The ASG software is integrated in the product. This is the case with Intuity AUDIX, release 5.X.
- ASG Guard. The ASG software resides on a separate box that sits on the network side of the product’s modem. The Guard houses its own modem, necessitating the disabling of the Intuity’s integral modem. ASG Guard is supported only with Intuity Release 4.4-7 and later; the use of ASG Guard isn’t supported with any earlier release. Also, ASG Guard isn’t supported with Definity AUDIX or R1 AUDIX. To my knowledge, ASG Guard isn’t available with Definity One either.

CHALLENGE – WHAT THE INTUITY SENDS
ASG utilizes a challenge/response mechanism to authenticate the caller. The ASG software (whether ASG Lock or Guard) generates a challenge and presents this challenge to the caller. The challenge is derived from the product id (also called the alarm id), and a digital secret key. The caller passes (via the connection tool) this challenge and the alarm id to an Avaya server (called the ASG Manager) that calculates the appropriate response to the challenge. This
response is then given to the Intuity as the replacement for a UNIX password. The Intuity ASG software then calculates the response in the same fashion as did the Avaya server and compares the two results. If they match, the caller is given a UNIX shell. Of course, if they don’t match, the caller is denied access.

For each attempted access, the Intuity will present a different seven-digit challenge. At present, the secret key doesn’t change (more on how this key may change later), and the alarm id doesn’t change but, the challenge is different each time you log in. (The customer can set parameters around time of day for their logins, but Avaya access will not be affected by these parameters.)

RESPONSE – WHAT THE CALLER SENDS

The caller must provide the correct response to the challenge in the time allotted; i.e., the Intuity will “timeout” if no response is received. (In testing, however, I found that after five minutes it still hadn’t timed out).

There are multiple methods to derive the correct response to an ASG challenge:

- **ASG Manager.** This is the aforementioned Avaya server. It resides on the Avaya LAN, and is programmed to include the alarm id of all Avaya ASG-equipped products. The ASG Manager is also known as a “token server,” as its purpose is to provide the correct “token” – or response – for a given challenge.
- **ASG Mobile.** This is a desktop Java-based desktop application that accesses the ASG Manager to provide the ASG response (or token). ASG Mobile is licensed to a particular user who is responsible for its safekeeping.
- **ASG Key.** This is a handheld device that can provide tokens for only those products it’s programmed for. Each ASG-protected login has a unique digital secret key. The ASG Key can only be programmed with one secret key. This is the tool that ASG customers will use.

ASG TOKEN SERVER

In the TSC, ASG Manager (accessed via Maestro or the “connect” tool) is the preferred method of accessing an Intuity with ASG protected ids. The INADS database administration group administers the ASG Managers (token servers). As Intuities are registered (during installation), the Intuity is assigned a unique alarm id (product id), and this id is programmed in the ASG Manager. Thus, the ASG Manager can generate the appropriate response to a challenge from a “registered” Intuity.

There are two ASG Managers on Avaya’s LAN - one serving as a backup.

ADMINISTERING ASG IN THE INTUITY

NOTE: This section applies to ASG Lock – the ASG software that’s co-resident with the Intuity software. Administration of ASG Guard is available at: [http://toolsa.bcs.lucent.com/~fxs/html/asgg.html](http://toolsa.bcs.lucent.com/~fxs/html/asgg.html).

ASG is enabled on a per-login id basis, and also on a per port basis. For the Avaya login ids to be ASG protected, ASG must be active on the com2 port. Following are instructions for administering ASG for **Avaya ids** only; i.e., the customer can enable ASG for their ids as well. First, we only enable ASG for the “tsc” login id! As of this writing, do not enable ASG for craft or nuucp.

There are three components to administering ASG on Intuity. In the order to be completed, they are:

- Alarm (or Product) id
- Enabling ASG for a particular login id
- Enabling ASG on a “com” port
Assigning the Alarm ID

Each Intuity leaves the factory with a default product id of 2000000000 (a 10-digit number beginning with ‘2’). Upon registration, the INADS group will change this product id to be a unique 10-digit number that begins with ‘2’. In the past, this id was used to identify this Intuity when it sent an alarm to INADS. The id still serves this purpose, but now has the additional role of seeding the ASG challenge. IMPORTANT: Never attempt to assign a product id; every Intuity in the world must have a unique id, so always let the INADS admin group assign the id! In INADS, the alarm id can be found in the configuration screen. The alarm id in the Intuity must match the id shown in INADS! The alarm id is found in the Intuity VEX screen: Customer Service/Administration Alarm Management

Enabling ASG for a Login Id

Use the Vex form:

ASG Security Administration  ASG security Login Administration

In the “Login id” field enter “tsc”
Enter ‘n’ in the “Access via ASG Blocked” field
Authentication type: ASG
System Generated Secret: ‘y’
Secret Key: leave blank

Press F2 (Create) to save.
You are about to modify the ASG user. Do you wish to continue (y/n)?
Type ‘y’ or press F1 (Yes)

Example: ‘tsc’ Administered For ASG

<table>
<thead>
<tr>
<th>User ID</th>
<th>Lev</th>
<th>Type</th>
<th>Blocked</th>
<th>Exp.date</th>
<th>#Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSC</td>
<td>05</td>
<td>PassKey</td>
<td>N</td>
<td>Unlimited</td>
<td>No Restrictions</td>
</tr>
</tbody>
</table>

Note the “type” of protection is “Passkey” not Password; indicating ASG is enabled for this id.

Example: ‘craft’ Administered For UNIX Password

<table>
<thead>
<tr>
<th>User ID</th>
<th>Lev</th>
<th>Type</th>
<th>Blocked</th>
<th>Exp.date</th>
<th>#Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRAFT</td>
<td>03</td>
<td>Password</td>
<td>N</td>
<td>Unlimited</td>
<td>No Restrictions</td>
</tr>
</tbody>
</table>

Administration privileges for this form are a hierarchical structure: tsc can change craft; craft can’t change tsc, and sa can’t change craft.

Enabling ASG for a com port

Use the Vex form:

ASG Security Port Administration Enable/Disable Security Validation for Dial In Ports

Example: ASG Enabled For COM Port 01

<table>
<thead>
<tr>
<th>Port Name /dev/tty01</th>
<th>Port Monitor Tag</th>
<th>Secure</th>
<th>Owner</th>
<th>/dev/tty00</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarm</td>
<td></td>
<td>YES</td>
<td>tsc</td>
<td></td>
<td>NO</td>
</tr>
</tbody>
</table>
EXAMPLE — SUCCESSFUL LOGIN USING ASG

Following is a successful attempt to login to an ASG-enabled Intuity:

voyager> connect "(303)538-6080" y tsc
Logging in as tsc

CTYPE=INAUD

Connecting to NTS ... OK
Getting a modem ... OK
Switch to Hayes mode ... OK
Modem "echo on" ... OK
Initializing modem speed to 28800
Serial Number: 04011592
Dialing 913053586079 ...
CONNECT 19200

MAIN: (303)538-6080
CUSTNAME: LUCENT TECHNOLOGIES
ADDRESS: 11900 N PECOS ST
CITY: WESTMINSTER STATE: CO
TYPE: INAUD FP: 100P ISSUE: CN44-5bb*23
PRODINFO=INAUD!100P!CN44-5bb*M23!A
PRODATA=!-7Y!LUCENT TECHNOLOGIES
CUSTID=(303)538-6080
DFMODE=n

Invoking prodtalk.

PRODUCT TALK subsystem - establishing connection.PRODINFO=INAUD!100P!CN44-5bb*M23!A!!
Connection established.
Type ~bye to exit.

INADS login started.

WARNING: Access to this system is restricted to authorized users for business purposes. Unauthorized access is a violation of the law. This service may be monitored for administrative and security reasons. By proceeding, you consent to this monitoring.

login:
WARNING: Access to this system is restricted to authorized users for business purposes. Unauthorized access is a violation of the law. This service may be monitored for administrative and security reasons. By proceeding, you consent to this monitoring.

login: tsc
Challenge: 659-2645   Product ID: 2205082380
Response:Calling TS asgmgr1
390-3483

UnixWare 2.1.3
driveit
Copyright 1996 The Santa Cruz Operation, Inc.  All Rights Reserved.
Copyright 1984-1995 Novell, Inc.  All Rights Reserved.
Copyright 1987, 1988 Microsoft Corp. All Rights Reserved.
U.S. Pat. No. 5,349,642
Last login: Mon May 24 08:00:22 1999 on term/01h

TERM=[at386]? 4425
Intuity driveitt%

TROUBLESHOOTING

What Should Happen
First, remember what should happen to allow a successful login:
- The connection tool retrieves from the INADS database the product’s alarm id
- The connection tool retrieves the ASG challenge from the product
- The connection tool sends these two elements to the ASG Manager, which in turn generates a response
- The connection tool sends the ASG response to the product
- The Intuity calculates a response, and compares it to the one supplied by the connection tool

The Default Product Id
To accommodate Intuity installations, the TSC connection tools can respond to a default product id. If the INADS record doesn’t have a product id, the connection tool will use the default id (10 digits, beginning with ‘2’). This id and the product’s challenge will be sent to the ASG Manager. (There’s also a means to specify to the connection tool the alarm id to be used. See the “connect” tool section below).

Are You Using The Right Tool?
Associates within the TSC must attempt connections to an ASG-enabled product using an ASG-capable tool. I.e., use TSCSS/Maestro or the “connect” tool on the toolsa UNIX server. These tools know the product is ASG-enabled, and “see” the ASG challenge. The connection tool retrieves from the INADS database the product’s alarm id and sends this alarm id, along with the ASG challenge, to the ASG Manager. The ASG Manager calculates a response, which the connection tool sends to the Intuity.

ASG MOBILE
ASG Mobile is a desktop tool that will allow you to “manually” answer to an ASG challenge. Essentially, you copy the product’s id and challenge into ASG Mobile, and it calculates the response which you then paste into the product’s response prompt.
For more information on ASG Mobile, go to:
http://info.dr.avaya.com/srvcs-rd/secure/ASG/

To obtain the tool, click on “Procedure to Acquire ASG Tools.”

**TSCSS/Maestro**

Ensure that the Intuity is responding with the same alarm id as shown in the INADS database. If not, is the Intuity sending the default (a 10-digit number beginning with ‘2’)? If so, look for old tickets that reflect a software reload. Once you’re sure you know how/why the id changed, and it’s okay to do so, change the product’s id to match the database (see the above section on product id administration). To successfully log in, you may need to use the procedures described below for the “connect” tool.

**“connect” tool**

This tool is available from the “toolsa” UNIX server. To get more information about “connect,” from the toolsa shell prompt, type “connect -?” or, “man connect | more”.

*Product Alarm id matches INADS alarm id*

To use connect in its basic form (i.e., the alarm id from the system matches the database) type:

```
connect "(NPA)nxx-xxxx" y tsc
```

The phone number shown is the INADS LDN not the main LDN and not the port (modem) number! This number is found on the INADS “configuration” screen. The ‘y’ denotes that the user will wait for a modem to become available (an ‘n’ works, too). The “tsc” is the login id to be used. Be sure to use the format shown, including the quotation marks, parentheses and the dash.

*Product Alarm id does not match INADS alarm id*

If the system reports an alarm id that is different from the database, use:

```
connect -a alarm_id -p modem_phone_number -t inaud -t sc -c p3nn8nt
```

where “alarm_id” is the one reported by the Intuity.

modem_phone_number is the phone number of the modem, not the INADS LDN
-t inaud identifies the target product as an Intuity
-t sc is the login id to use (Preceding the login id is an ell)
-c password This is the UNIX password for the ‘tsc’ login id.

**Try Another Login Id**

If you’re unable to respond successfully to an ASG challenge, try logging with a login id that’s not ASG protected. Try using connect or “cu” to login as “craft.” To use connect, type:

```
connect -p modem_phone_number -l craft -t inaud -c password
```

(Preceding the login id – craft – is an ell).

The ability to login as craft will allow you to reload the ASG software – see the section below on [reloading ASG software.](#)

**Changing The Product’s Alarm Id**

If the product is responding with an alarm id other than the database shows and, it’s not the default id, inquire if software has been reloaded at the customer site. Be careful here, as this is an unusual situation… possibly this system
has been reloaded using software from another system? To successfully log in, you may need to use the procedures described above for the "connect" tool.

**Contact The INADS Database Administration Group**

Have this group check to ensure the ASG Managers have the product’s alarm id loaded. It’s probably also useful to ensure you can access other ASG-protected Intuities (another Release 5.0 system).

**Specific Faults**

- No Response from Product Modem  
  The addition of ASG didn’t impact this. Use traditional troubleshooting techniques.
- No Login prompt  
  The addition of ASG didn’t impact this. Use traditional troubleshooting techniques.
- No ASG Challenge. I.e., you received a password prompt.  
  Log in and check that ASG is active for the port and login id that you used.
- No Product Alarm id or wrong id  
  Assign to the Intuity the alarm id shown in INADS
- ASG Token Server didn’t respond  
  Escalate to the INADS database administration group.
- Failed to login to ASG Manager (token server)  
  Escalate to the INADS database administration group.
- Intuity didn’t accept ASG response  
  Verify that the product and INADS alarm ids match.
  Escalate to the INADS database administration group to verify the servers are up and programmed correctly.
  See below for reloading/recovering ASG software
  Escalate to the next Intuity step
- Alarm id mismatch between product and INADS  
  Escalate to the INADS database administration group to verify the servers are up and programmed correctly.
  See the below step for reloading/recovering ASG software
  Escalate to the next Intuity step

**RECOVERING ASG FROM CUSTOMER BACKUP**

The ASG default secret key and alarm id are backed up nightly. It might be necessary to first reload the ASG software – see below. (I’ll update this document once I know the specific commands used to recover just the ASG files.)

**RELOADING ASG SOFTWARE**

With the Release 5.0 CD in the drive, it’s possible to remotely reload the ASG package. Either the craft or tsc login id can be used. First, remove the ASG package, then add the ASG package. Next, restore from the customer’s backup. (I’ll add more once I know the specific package names, etc.) Verify that the alarm id matches the id found in INADS.

**CUSTOMER USE OF ASG**

Customers desiring an ASG challenge for their login ids – “sa” and/or ‘vm” - must enable ASG for each id for which they desire a challenge. See the above section for assistance in the necessary administration. Please see the topics below to avoid customer misunderstandings of the ASG technology.
Enabling ASG on Customer Login ids

There have been a number of instances where customers did not understand that ASG challenges are available for the "sa" and "vm" login ids. Any Release 5.0 or later Intuity can generate ASG challenges for the customer’s ids. For Intuities prior to Release 5, an ASG Guard is required.

To avoid using multiple secure tokens

A related misunderstanding is that customers feel they need a separate ASG Key (the hand-held, key-chain device) for each ASG-protected product – not at all a desirable situation when you have dozens of ASG-protected products. To avoid using multiple keys, but still have the benefit of ASG challenge/response, customers are installing ASG Guards in front of Release 5 Intuities. This accomplishes the intent, but at extra customer expense.

The need for ASG Guard or multiple keys can be avoided if all ASG-protected products utilize the same secret key. Referring back to the section entitled "CHALLENGE – WHAT THE INTUITY SENDS," the secret key is used to generate the challenge and to validate the ASG response. As an example, assume the customer has a Release 5 Intuity and an R9 Definity switch. To access either device using the same ASG Key, the switch, the Intuity and the key must all use the same secret key.

Looking at the Enabling ASG for a Login Id section one more time, you’ll see the Intuity has two fields that we’ve ignored until now: “System Generated Secret” and “Secret Key.” In our example, the customer would administer the key to use the same secret key as the switch. What’s left is to administer the Intuity to use the same secret key as the switch. The “System Generated Secret” field is changed to “No” and the secret key from the switch is copied into the “Secret Key” field. (In Definity switch, the secret key is found on page 2 of the login administration form [“disp login cust1”] for example). Page 2 will only appear if, at the bottom of page 1, the “Access Security Gateway” field is set to “y” [yes]. On page 2, the secret key is found in the “Secret Key” field.)

Using ASG Guard and ASG Lock

Caveat: I’m only familiar with Intuity… I don’t know if it’s possible to place a guard in front of other Avaya products that use ASG lock.

It is possible to place an ASG Guard in front of an Intuity that uses ASG Lock (Release 5 or later). Assume that, for security purposes, a customer wishes to be challenged twice when accessing the Intuity. By connecting the Intuity release 5 system to the ASG guard, and administering the Intuity to enable ASG for the customer login ids, the customer will receive two challenges. (Assuming that token, the guard and the Intuity all utilize the same secret key, then one token will successfully answer both challenges).

In this instance, the TSC personnel attempting to access the Intuity will also be challenged twice. The “connect” tool was written to handle this, although, to my knowledge, it’s not widely advertised. If two challenges aren’t desirable when using Avaya ids, use the Intuity administration forms and disable ASG for the “tsc” login id. In this manner, the only challenge will originate from the guard.

ASG Guard and the RMB

When used with the Intuity, the ASG Guard will replace the on-board RMB modem. The ASG Guard must connect to the RMB port, not a com port. If the customer wants to be challenged when remotely accessing to the Intuity, equip the guard with two modem numbers; one for the customer, one for Avaya.

ASG Guard is only supported with Intuity 4.4-7 or later and, the RMB must be running 1.4 or later software for ASG Guard to work.
ASG KEY CHANGER
In the future, the expert system will utilize an ASG Key Changer – software that will change, on a periodic basis, the ASG secret key that’s resident on the customer’s disk. This secret key is backed up nightly, so, recovering should be similar to the procedures described in the above troubleshooting section.

WHERE TO GET MORE INFORMATION

ASG Used With Intuity
The Intuity documentation has ASG information in the system administration section, and also, in the security section. This documentation is available through EDOC.

ASG Operational Guidelines
The ASG Operational Guidelines is available through EDOC.

ASG Web Page
http://info.dr.avaya.com/srvcs-rd/secure/