

## Microsoft Intelligent Application Gateway Installation Notes

### Table of Contents

Microsoft Intelligent Application Gateway Installation Notes .....	1
1. Introduction .....	1
2. Prerequisites .....	1
3. Special Considerations .....	1
4. Installation .....	2
4.1. Edit the Configuration Files .....	2
4.2. Copy the Configuration files .....	2
4.3. Configure the IAG .....	3
4.3.1. Create an ISA rule to allow access from the IAG to the PINsafe server .....	3
4.3.2. Configure Login Page: .....	3
4.3.3. Active Directory with XML or RADIUS authentication .....	4
4.3.4. Configuring RADIUS authentication (when not using XML) .....	4
4.3.5. Configuring XML authentication (when not using RADIUS) .....	5
4.3.6. Configuring the URL rewriting rules .....	6
4.4. Configure The PINsafe Server .....	8
5. Testing .....	8
6. Troubleshooting .....	8
7. Additional Information .....	9

## 1. Introduction

This configuration document outlines how to integrate PINsafe with Microsoft Intelligent Application Gateway using Active Directory authentication in addition to the PINsafe authentication. This configuration uses XML to communicate with the PINsafe server.

If installing PINsafe on an IAG appliance it may be required to install PINsafe to use a different port than the default 8080.

## 2. Prerequisites

Microsoft Intelligent Application Gateway 3.7  
IAG and URL rewriting documentation  
PINsafe server with ChangePIN  
ChangePIN configuration document

## 3. Special Considerations

If upgrading the IAG to a higher service pack (e.g. sp2), the configuration files, particularly login.asp may be overwritten. Verify the files after an upgrade. Also note that the URL rewriting rules may differ from version to version, so these should also be verified.

## 4. Installation

### 4.1. Edit the Configuration Files

1. Edit the file Token.inc with the required shared secret and to represent the PINsafe server IP address and PINsafe install name:

```
m_secret = "secret"
```

```
objWinHttp.Open "GET", "https://192.168.1.1:8443/proxy/AgentXML?xml=" &  
m_request, false
```

Note for a software install of PINsafe not using SSL or an older appliance this should be:

```
objWinHttp.Open "GET", "http://192.168.1.1:8080/pinsafe/AgentXML?xml=" &  
m_request, false
```

2. Edit the file Portalname1postpostvalidate.inc to represent the PINsafe server IP address and changePIN install name:

```
'response.redirect "https://192.168.1.1:8443/changepin"  
g_orig_url = "https://192.168.1.1:8443/changepin"
```

Note for a software install of PINsafe not using SSL or an older appliance this should be:

```
response.redirect "http://192.168.1.1:8080/changepin"  
g_orig_url = "http://192.168.1.1:8080/changepin"
```

3. Edit the file images.asp with the required shared secret and to represent the PINsafe server IP address and PINsafe install name:

```
objWinHttp.Open "GET",  
"https://192.168.1.1:8443/proxy/SCImage?username=" & request.querystring("username"), false
```

Note for a software install of PINsafe not using SSL or an older appliance this should be:

```
objWinHttp.Open "GET",  
"http://192.168.1.1:8080/pinsafe/SCImage?username=" & request.querystring("username"), false
```

### 4.2. Copy the Configuration files

1. Copy Token.inc and Portalname1postpostvalidate.inc to: <path to IAG install>\von\InternalSite\inc\CustomUpdate

2. Copy login.asp file to: <path to IAG install>\von\InternalSite\CustomUpdate
3. Copy images.asp to: <path to IAG install>\von\InternalSite\Images\CustomUpdate

### 4.3. Configure the IAG

#### 4.3.1. Create an ISA rule to allow access from the IAG to the PINsafe server

On the ISA configuration select New Access Rule and create a rule to allow traffic from the IAG to the PINsafe server.

Port 8443 (or port 8080 for software installs, older appliances and when using XML authentication)

From Local Host (i.e. the IAG)

To PINsafe Server (or Internal Network)

Outbound Traffic

#### 4.3.2. Configure Login Page:

Select the IAG Configuration GUI, From the Advanced Trunk Configuration select Authentication and set the Login Page to customupdate\Login.asp

**Advanced Trunk Configuration [portal]**

Application Access Portal | URL Inspection | Global URL Settings | URL Set

General | **Authentication** | Session | Application Customization

☒ **Authenticate User on Session Login**

Select Authentication Servers:

AD	
Token	

Add... Remove

↑ ↓

☐ User Selects From a List of Servers

☒ Show Server Names

☒ User Must Provide Credentials for Each Selected Server

☒ Use the Same User Name

☐ Use Integrated Windows authentication

☒ Enable NTLM protocol

☒ Enable Kerberos protocol

☒ Enable Users to Add Credentials On-the-Fly

☒ Enable Users to Change Their Passwords

☐ Notify User  Days Prior to Expiration

☒ Enable Users to Manage Their Credentials

☒ Enable Users to Select Language

☐ Skip client compliance checks when accessing a SharePoint site outside of a session

Login Page:

On-the-Fly Login Page:

Permitted Authentication Attempts:

Block Period:  Minutes

☒ **Logoff Scheme**

Logoff URL:

Logoff Message:

Wait  Sec. After Logoff URL to Terminate Session

☐ Pass the Logoff to the Application Server

☐ Send Logoff Response to Browser

OK Cancel

### **4.3.3. Active Directory with XML or RADIUS authentication**

When using PINsafe as a secondary authentication such as with Active Directory, ensure that the options for secondary authentication are selected.

The IAG can be configured to use RADIUS or XML authentication. XML authentication allows extra functionality such as checking the users PIN number expiration.

Note that when using a PINsafe appliance with a proxy configured, the XML requests need to be made to the <https://<IP>:8080/pinsafe> address rather than the proxy address. This applies currently to all PINsafe versions.

### **4.3.4. Configuring RADIUS authentication (when not using XML)**

To enable RADIUS authentication create a repository of type “RADIUS” on the IAG configuration.

To use RADIUS do the following-

1. Access the IAG configuration GUI.
2. Click on Admin Authentication Users/Group repository
3. Select New to create a new repository
4. In the drop down menu, select “RADIUS” and in the Name field enter PINsafe RADIUS
5. Enter the IP of the PINsafe server
6. Enter port 1812
7. If required enter a second IP/port
8. Enter a shared secret key of the same value as the PINsafe server
9. Click on Add and apply this repository to the relevant trunk.
10. Ensure User must enter credentials for each server is selected.
11. If AD password is to be entered ensure that an AD authentication server is specified.
12. Activate the configuration
13. Configure PINsafe as a RADIUS server

**Add Server**

Type: RADIUS

Name: PINsafe RADIUS

IP/Host: 192.168.9.45

Port: 1812

Alternate IP/Host: 192.168.9.46

Alternate Port: 1812

Secret Key: xxxxxx

☐ Support Challenge Response

☐ Use a Different Server for User/Group Authorization

Select Server: Built-In Users/Groups

☐ Extract User's Groups from RADIUS Attribute

Attribute Type: 25

Attribute Format: ou=<group>

Help OK Cancel

#### 4.3.5. Configuring XML authentication (when not using RADIUS)

To enable the token.inc file, create a repository of type “Other” on the IAG configuration. The repository you create must match the name of the file (ie, if the inc file is called Token.inc, the repository must be named Token).

To create the repository, do the following-

1. Access the IAG configuration GUI.
2. Click on Admin Authentication Users/Group repository
3. Select New to create a new repository
4. In the drop down menu, select “Other” and in the Name field type in the name of the inc file (See screen shot below)
5. Click on Add and apply this repository to the relevant trunk.
6. Activate the configuration



#### 4.3.6. Configuring the URL rewriting rules

To allow access to the image.asp

1. Select the required Trunk
2. Select Configure from the Advanced Trunk Configuration
3. Select the 'URL Set' Tab
4. Add a rule to permit access to the image.asp

Portal\_InternalSite\_Rule##

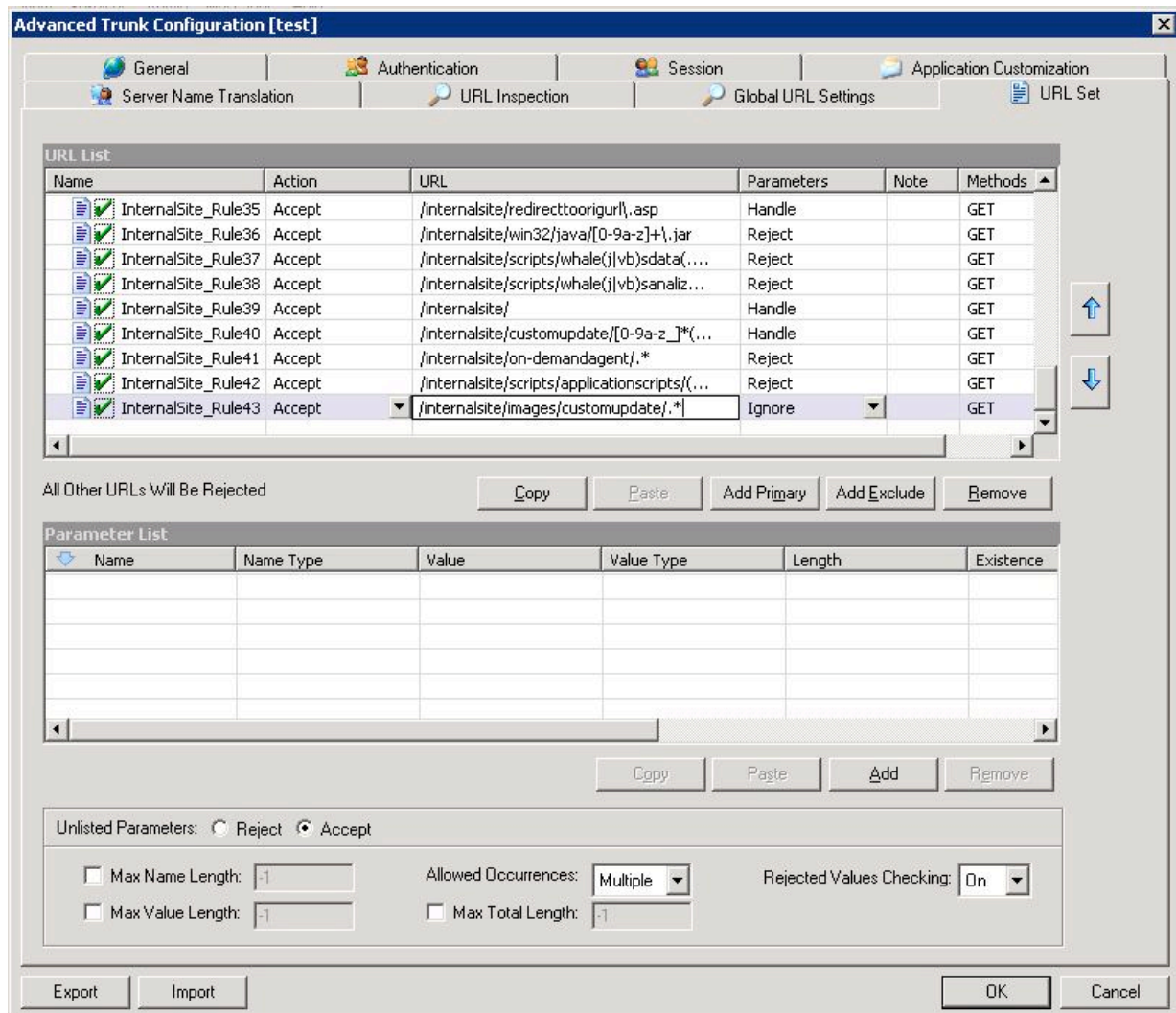
With parameters of:

Action: Accept

URL: /internalsite/images/customupdate/.\*

Parameter: Ignore (i.e. ignore any parameters)

Method: Get



Edit Rule to allow Access to the postvalidate.asp

1. Select the postvalidate.asp rule (Usually Internal\_Rule2)
2. Under Parameters select Ignore

Alternatively add the following to the parameters list:

Turing  
SMS

To allow access to the ChangePIN application

3. Select the required Trunk
4. Under Applications select Add
5. Step 1: Click the Web Applications Radio App and Generic Web App then Next
6. Step 2: Enter Application name ChangePIN and Application Type: pinsafe then Next
7. Step 3: Enter the ChangePIN IP address, and under path the location of the ChangePIN install normally changepin, set the port to 8080, then Next
8. Step 4: Select Next
9. Step 5: Check details are correct, specifically http://<IP Address>:8443/changepin and then Finish

NOTE: If changing the IP address then change the IP address in the Application Properties on the Web Servers and the Portal Applications tabs.

#### **4.4. Configure The PINsafe Server**

Configure a PINsafe Agent

1. On the PINsafe Management Console select Server/Agent
2. Enter a name for the Agent
3. Enter the IAG internal IP address
4. Enter the shared secret
5. Click on Apply to save changes

Configure a RADIUS NAS entry (if using RADIUS)

1. Ensure the RADIUS server is running on PINsafe
2. On the PINsafe Management Console select RADIUS NAS
3. Enter a name for the NAS
4. Enter the IAG internal IP address
5. Enter the shared secret
6. Click on Apply to save changes

Configure Single Channel Access

1. On the PINsafe Management Console select Server/Single Channel
2. Ensure 'Allow session request by username' is set to YES

### **5. Testing**

Browse to the login page, select Turing and enter a username, the Turing image should appear. Test using the SMS option. Check for requests on the PINsafe server.

Successful RADIUS authentication

The following user logged into trunk "test" (secure=0): User: admin; Source IP: 192.168.9.87; Authentication Server: PINsafe RADIUS; Session: B9FCC62A-B073-445D-9AAE-2FB1109EE5E6.

### **6. Troubleshooting**

Check the PINsafe server logs and system event logs for any errors or lack of communication as well as the IAG logs under Admin/Web Monitor. Check the ISA server logs.

URL blocking by the IAG

Request failed, the URL contains an illegal path. Trunk: test; Secure=0; Application Name: Whale Internal Site; Application Type: InternalSite; Rule: Default rule; Source IP: 192.168.9.87; Method: GET; URL: /InternalSite/Images/customupdate/images.asp?username=admin.

From a web browser on the IAG check to see if it is possible to generate a Turing image <https://<IP address of PINsafe server>:8443/proxy/SCImage?username=test>

for older appliances and software installs not using SSL;  
<http://<IP address of PINsafe server>:8080/pinsafe/SCImage?username=test>

## **7. Additional Information**

For assistance in the PINsafe installation and configuration please contact your reseller or email Swivel Secure support at [support@swivelsecure.com](mailto:support@swivelsecure.com)