PINsafe®

Microsoft Intelligent Application Gateway Installation Notes

Created May 2007

Table of Contents

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.

Prerequisites

Microsoft Intelligent Application Gateway 3.7
PINsafe server with ChangePIN
ChangePIN configuration document
PINsafe Active Directory Configuration Document

Installation

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: Also make sure the port is different than 8080.

   ```
   m_secret = "secret"

   objWinHttp.Open "GET", "http://127.0.0.1:8180/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 "http://127.0.01:8180/changepin"
   g_orig_url = "http://127.0.0.1:8180/changepin"
   ```

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

   ```
   objWinHttp.Open "GET", "http://127.0.0.1:8180/pinsafe/SCImage?username="&request.querystring("username"), false
   ```

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
3. Copy image.asp to: <path to IAG install>\von\InternalSite\Images\CustomUpdate

Configure the IAG

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

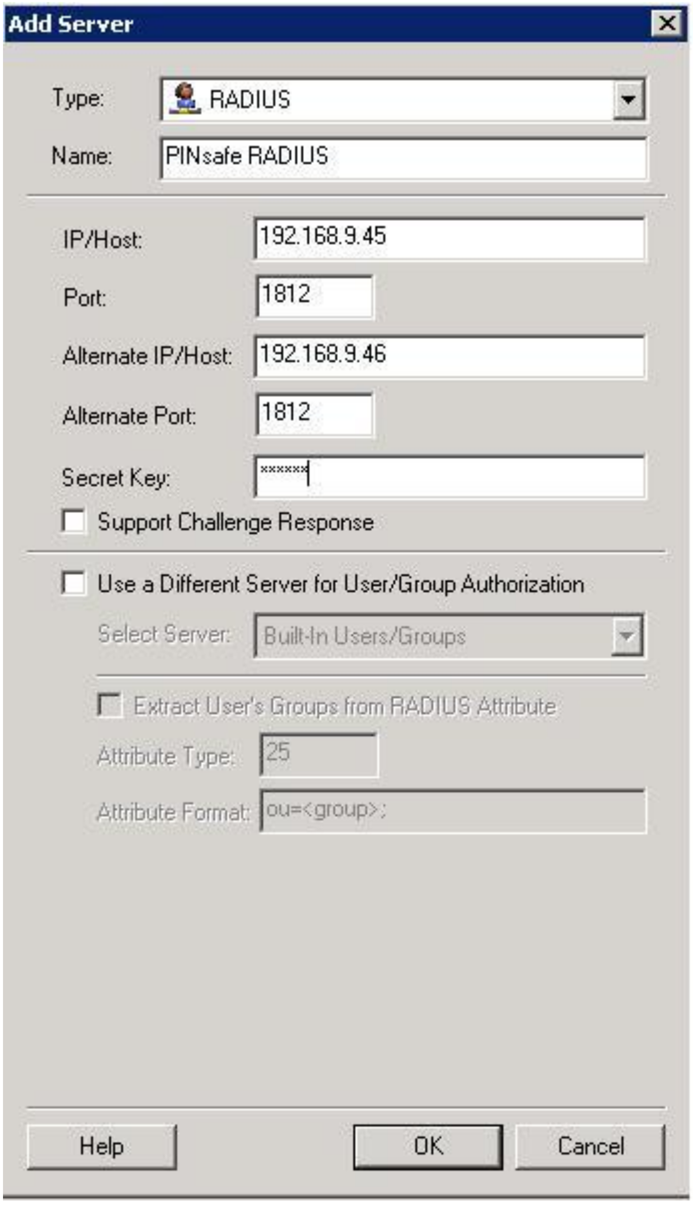
Configuring RADIUS authentication (when not using XML)

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. Activate the configuration
11. Configure PINsafe as a RADIUS 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: ******
□ 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>;

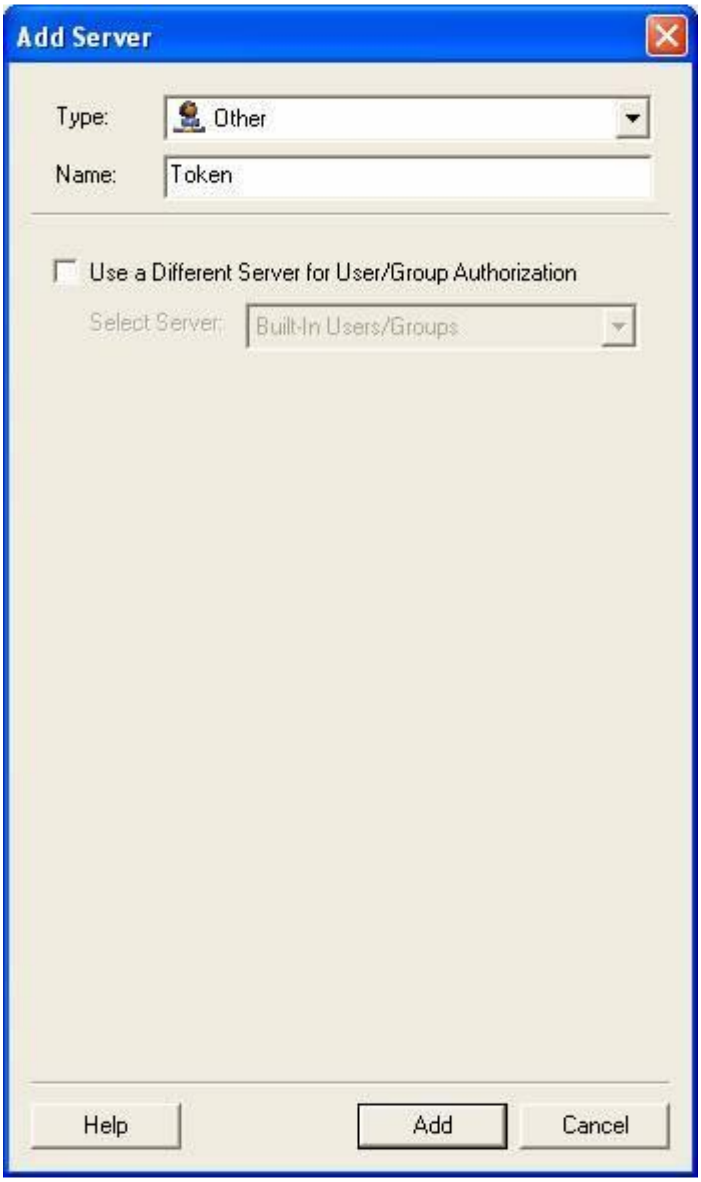
Configuring XML authentication (when not using RADIUS)

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



Add Server

Type: Other

Name: Token

□ Use a Different Server for User/Group Authorization

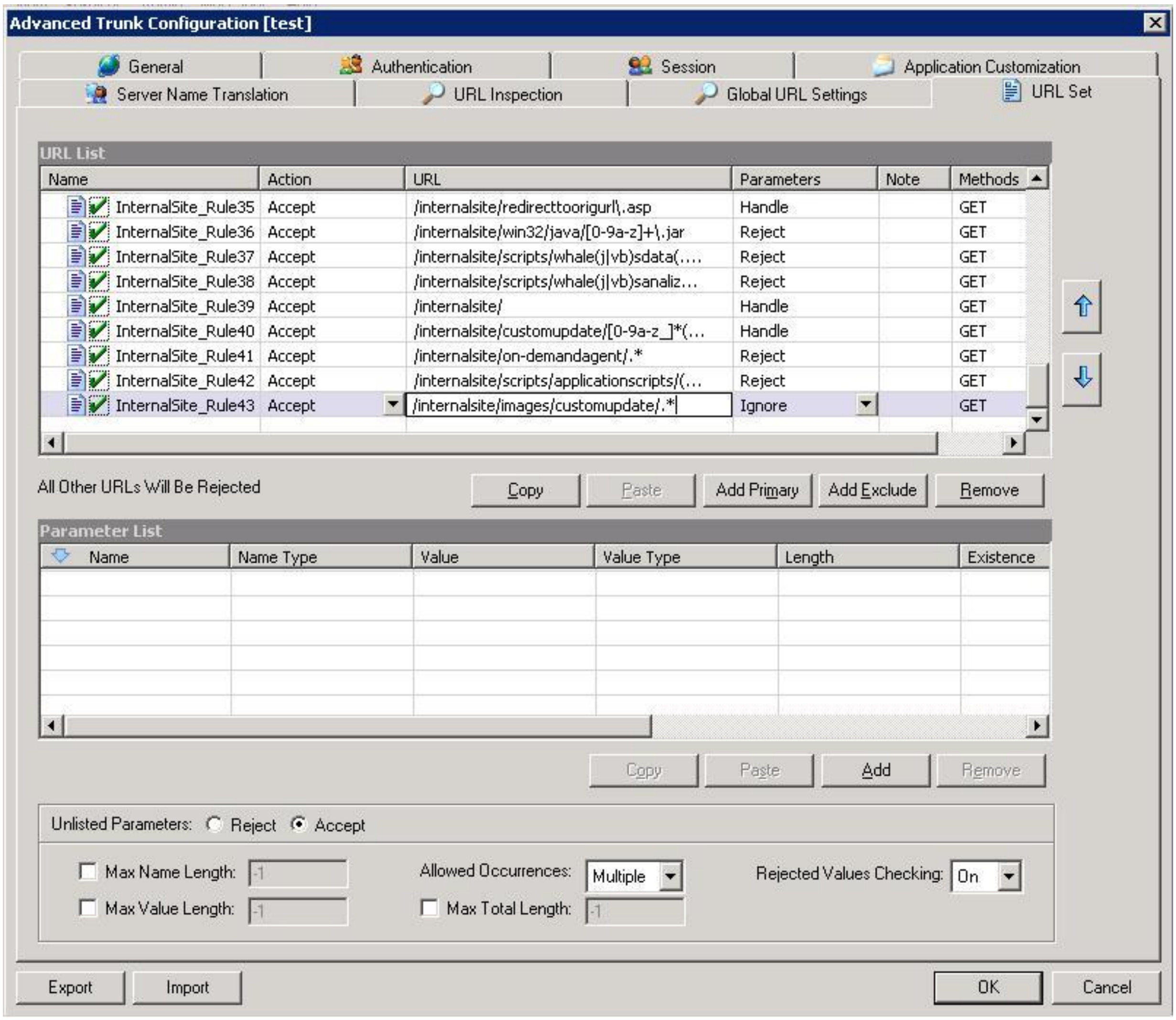
Select Server: Built-In Users/Groups

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



URL List

Name	Action	URL	Parameters	Note	Methods
InternalSite_Rule35	Accept	/internalsite/redirecttoorigurl\.asp	Handle		GET
InternalSite_Rule36	Accept	/internalsite/win32/java/[0-9a-z]+\.jar	Reject		GET
InternalSite_Rule37	Accept	/internalsite/scripts/whale(j|vb)sdata(....	Reject		GET
InternalSite_Rule38	Accept	/internalsite/scripts/whale(j|vb)sanaliz...	Reject		GET
InternalSite_Rule39	Accept	/internalsite/	Handle		GET
InternalSite_Rule40	Accept	/internalsite/customupdate/[0-9a-z_]*(...	Handle		GET
InternalSite_Rule41	Accept	/internalsite/on-demandagent/.*	Reject		GET
InternalSite_Rule42	Accept	/internalsite/scripts/applicationscripts/(...	Reject		GET
InternalSite_Rule43	Accept	/internalsite/images/customupdate/.*	Ignore		GET

All Other URLs Will Be Rejected

Parameter List

Name	Name Type	Value	Value Type	Length	Existence

Unlisted Parameters: ○ Reject ● Accept

□ Max Name Length: -1
□ Max Value Length: -1
Allowed Occurrences: Multiple
□ Max Total Length: -1
Rejected Values Checking: On

To allow access to the ChangePIN application

1. Select the required Trunk
2. Under Applications select Add
3. Step 1: Click the Web Applications Radio App and Generic Web App then Next
4. Step 2: Enter Application name ChangePIN and Application Type: pinsafe then Next
5. 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
6. Step 4: Select Next
7. Step 5: Check details are correct, specifically http://<IP Address>:8080/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.

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

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.
```

Troubleshooting

Check the PINsafe server logs and system event logs for any errors or lack of communication as well as the IAG 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.
```

Additional Information

For assistance in the PINsafe installation and configuration please contact support at support@nappliance.com