

# Microsoft UAG Integration

## Contents

- 1 Introduction
- 2 Prerequisites
- 3 Baseline
- 4 Architecture
- 5 Installation
  - ◆ 5.1 Configure The Swivel Server
    - ◇ 5.1.1 Configure a RADIUS NAS entry
    - ◇ 5.1.2 Configure Single Channel Access
  - ◆ 5.2 Configure the UAG
    - ◇ 5.2.1 Edit the UAG Configuration Files
    - ◇ 5.2.2 Copy the Configuration files
    - ◇ 5.2.3 Configure the TMG
    - ◇ 5.2.4 Configure Login Page
    - ◇ 5.2.5 RADIUS authentication Configuration
    - ◇ 5.2.6 Configuring the URL rewriting rules
- 6 Verifying the Installation
- 7 Troubleshooting
- 8 Additional Configuration Options
  - ◆ 8.1 RADIUS Challenge and Response
  - ◆ 8.2 PINpad Integration
  - ◆ 8.3 ChangePINpad Integration
  - ◆ 8.4 Button size and aspect ratio
  - ◆ 8.5 XML Authentication
- 9 Known Issues and Limitations
- 10 Additional Information

## Introduction

This configuration document outlines how to integrate Swivel with Microsoft Forefront Unified Access Gateway using Active Directory authentication in addition to the Swivel authentication.

If installing Swivel on the UAG appliance it may be required to install Swivel to use a different port than the default 8080.

## Prerequisites

Microsoft Forefront Unified Access Gateway

UAG and URL rewriting documentation

Swivel 3.x server with ChangePIN

ChangePIN configuration document

The following files are required to be uploaded to the UAG

images.asp

login.asp (Rename loginturingsms.asp as login.asp)

Portalname1postpostvalidate.inc

Token.inc

The files can be downloaded from here: [UAG Files](#)

UAG Update 1 requires a modified login page, this additional file can be downloaded here: [UAG Update 1 Files](#)

UAG SP1 through to SP4 requires modified login pages, the complete set of files can be downloaded here: [UAG SP1 Files](#)

[UAG SP1 through to SP4 SMS only request button login](#) also [UAG SP1 through to SP4 TURing only request button login](#)

[RADIUS ChangePIN](#) for UAG, backup then replace the file LoginContinue.asp

## Baseline

Microsoft Forefront Unified Access Gateway 1.0.1101.0

Swivel 3.5

## Architecture


The UAG makes authentication requests against the Swivel server by RADIUS or XML.

## Installation

### Configure The Swivel Server

#### Configure a RADIUS NAS entry

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

**RADIUS>NAS** 

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the authentication server via the RADIUS interface.

NAS: Identifier:	<input type="text" value="Device Name"/>
Hostname/IP:	<input type="text" value="192.168.0.1"/>
Secret:	<input type="password" value="•••••"/>
EAP protocol:	<input type="text" value="None"/>
Group:	<input type="text" value="---ANY---"/>
Authentication Mode:	<input type="text" value="All"/>
Change PIN warning:	<input type="text" value="No"/>

#### Configure Single Channel Access

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

## Server>Single Channel

Please specify how single channel security strings are delivered.

Image file:	<input type="text" value="turing.xml"/>
Rotate letters:	<input type="text" value="No"/>
Allow session request by username:	<input type="text" value="Yes"/>
Only use one font per image:	<input type="text" value="Yes"/>
Jiggle characters within slot:	<input type="text" value="No"/>
Add blank trailer frame to animated images:	<input type="text" value="Yes"/>
Text Alpha Value:	<input type="text" value="80"/>
Number of complete display cycles per image:	<input type="text" value="10"/>
Inter-frame delay (1/100s):	<input type="text" value="40"/>
Image Rendering:	<input type="text" value="Static"/>
Multiple Authentications per String:	<input type="text" value="No"/>
Generate animated images:	<input type="text" value="No"/>
Random glyph order when animating:	<input type="text" value="No"/>
No. Characters Visible:	<input type="text" value="1"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

### Configure the UAG

#### Edit the UAG Configuration Files

Edit the file images.asp with the below URL to represent the Swivel server IP address and Swivel install name:

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

Where <hostname\_of\_pinsafe> is your Swivel server hostname.

Then edit Token.inc with the required shared secret:

```
m_secret = "<secret>"
```

Where <secret> is your secret (do not enter the angle brackets).

#### Copy the Configuration files

Note: Ensure any existing files are backed up first.

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

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

### **Configure the TMG**

Create a Threat Management Gateway rule to allow access from the UAG to the Swivel server

On the TMG configuration select New Access Rule and create a rule to allow traffic from the UAG to the Swivel server.

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

From Local Host (i.e. the UAG)

To Swivel Server (or Internal Network)

Outbound Traffic

### **Configure Login Page**

Select the UAG Configuration GUI, From the Advanced Trunk Configuration select Authentication and set the Login Page to customupdate\Login.asp. This can be changed to reflect a different install location or trunk.

**Advanced Trunk Configuration [portal]**

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

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

### RADIUS authentication Configuration

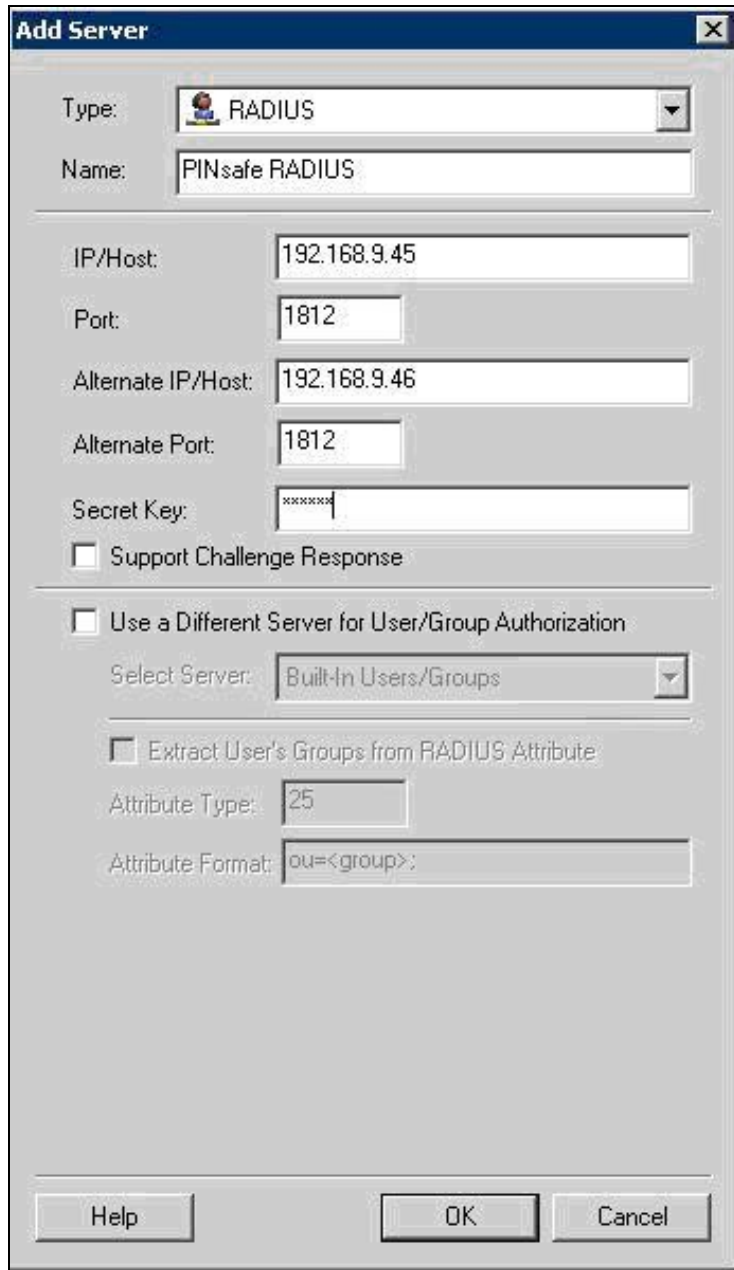
Swivel can be configured as the Primary authentication server or more usually is configured as a secondary authentication server. When using Swivel as a secondary authentication such as with Active Directory, ensure that the options for secondary authentication are selected.

To enable RADIUS authentication create a repository of type ?RADIUS? on the UAG configuration.

To use RADIUS do the following-

1. Access the UAG 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 Swivel RADIUS
5. Enter the IP of the Swivel server. Note, when using a Swivel HA pair, do not use the VIP address for RADIUS authentication, but use the real IP address.

6. Enter port 1812
7. If required enter a second IP/port
8. Enter a shared secret key of the same value as the Swivel 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 Swivel as a RADIUS server



The image shows a Windows-style dialog box titled "Add Server". It contains several input fields and checkboxes for configuring a RADIUS server. The "Type" dropdown is set to "RADIUS". The "Name" field contains "PINsafe RADIUS". The "IP/Host" field contains "192.168.9.45", "Port" contains "1812", "Alternate IP/Host" contains "192.168.9.46", and "Alternate Port" contains "1812". The "Secret Key" field contains "xxxxxx". There are three checkboxes: "Support Challenge Response" (unchecked), "Use a Different Server for User/Group Authorization" (unchecked), and "Extract User's Groups from RADIUS Attribute" (unchecked). The "Select Server" dropdown is set to "Built-In Users/Groups". The "Attribute Type" field contains "25" and the "Attribute Format" field contains "ou=<group>:". At the bottom are "Help", "OK", and "Cancel" buttons.

**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**

### Configuring the URL rewriting rules

To allow access to the images.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 images.asp

InternalSite\_Rule100

Note: This must be named InternalSite\_Rule, example: InternalSite\_Rule100 (use a high number to prevent it being overwritten by updates)

With parameters of:

Action: Accept

URL: /internalsite/images/customupdate/images.asp

Note: You can use /internalsite/images/customupdate/\* for testing, and add additional rules to check the input.

Parameter: Handle (i.e. handle any parameters. For troubleshooting it may be useful to set this to ignore).

Method: Get

To Allow access to Swivel specific parameters:

Under Parameters select Add, add the following values:

Parameter 1:

- Name: username
- Name Type: String
- Value: ?[a-z0-9]+? (this is a basic regex and may need changing depending on the users username policy)
- Value Type: String
- Length: 1:100 (may need to up 100 depending on customer username length)
- Existence: Mandatory
- Occurrences: Single
- Max total length: -1
- Rejected values checking: on

Parameter 2:

- Name: random
- Name Type: String
- Value Type: Integer
- Existence: Optional
- Occurrences: Single
- Max total length: -1
- Rejected values checking: on

**Advanced Trunk Configuration [test]**

General Authentication Session Application Customization

Server Name Translation URL Inspection Global URL Settings

**URL List**

Name	Action	URL	Parameters	Note	Methods
InternalSite_Rule35	Accept	/internalsite/redirecttoorigurl\. <td>Handle</td> <td></td> <td>GET</td>	Handle		GET
InternalSite_Rule36	Accept	/internalsite/win32/java/[0-9a-z]+\. <td>Reject</td> <td></td> <td>GET</td>	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

Copy Paste Add Primary Add Exclude Remove

**Parameter List**

Name	Name Type	Value	Value Type	Length	Existence

Copy Paste Add Remove

Unlisted Parameters: ☐ Reject ☒ Accept

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

Export Import OK

Edit Rule to allow Access to the validate.asp

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

Alternatively add the following to the parameters list:

Turing

SMS

To Allow access to Swivel specific parameters:

Select the InternalSite\_Rule2

Under Parameters select Add, add the following values:

Name: swivel



Name Type: String

Value:

Value Type: String

Length: 1:100

Existence: Optional

Occurrences: Multiple

Max total length: -1

Rejected values checking: on

Also add a Parameter with the following values:

Name: orig\_url

Name Type: String

Value:

Value Type: String











Length: 1:200

Existence: Optional

Occurrences: Multiple

Max total length: -1

Rejected values checking: on

URL list				
Name	Action	URL	Param	
 Portal_Rule12	Accept	/({secure}?[^\s]+portalhomepage/scripts/(limitedportal toolbarsec...	Reject	
 InternalSite_Rule1	Accept	/internalsite/(owa/)?(customupdate/)?login\,asp	Handle	
 InternalSite_Rule2	Accept	/internalsite/validate\,asp	Handle	
 InternalSite_Rule3	Accept	/internalsite/(sessiontimeout scheduledlogoff postvalidate pas...	Reject	
 InternalSite_Rule4	Accept	/internalsite/setpolicy\,asp	Handle	
 InternalSite_Rule5	Accept	/internalsite/validatecontinue\,asp	Handle	
 InternalSite_Rule6	Accept	/internalsite/validatechooseuser\,asp	Handle	
 InternalSite_Rule7	Accept	/internalsite/credentialssettings\,asp	Handle	
 InternalSite_Rule8	Accept	/internalsite/loginchange-password\,asp	Handle	
 InternalSite_Rule9	Accept	/internalsite/validatechannelpassword\,asp	Handle	

All other URLs will be rejected.

Parameter list						
Name	Name Type	Value	Value Type	Length	Existence	Occurrences
secure	String	[01]	String	1	Optional	Single
site_name	String	[0-9a-z]+	String	100	Optional	Single
site_redirector	String	[^\s"']*	String	0:256	Optional	Single
swivel	String		String	1:100	Optional	Multiple
trusted	String	[014]	String	0:1	Optional	Single
user_name	String	[^*0]*	String	0:350	Optional	Multiple

**URL list**

Name	Action	URL	Param...
Portal_Rule12	Accept	/secure)?[^\]+portalhomepage/scripts/(limitedportal toolbarsc...	Reject
InternalSite_Rule1	Accept	/internalsite/(owa/)?(customupdate/)?login\,asp	Handle
InternalSite_Rule2	Accept	/internalsite/validate\,asp	Handle
InternalSite_Rule3	Accept	/internalsite/(sessiontimeout scheduledlogoff postvalidate pas...	Reject
InternalSite_Rule4	Accept	/internalsite/setpolicy\,asp	Handle
InternalSite_Rule5	Accept	/internalsite/validatecontinue\,asp	Handle
InternalSite_Rule6	Accept	/internalsite/validatechooseuser\,asp	Handle
InternalSite_Rule7	Accept	/internalsite/credentialssettings\,asp	Handle
InternalSite_Rule8	Accept	/internalsite/loginchangeppassword\,asp	Handle
InternalSite_Rule9	Accept	/internalsite/validatechannepassword\,asn	Handle

All other URLs will be rejected.

Copy Paste Add Primary Add Exclude Remove

**Parameter list:**

Name	Name Type	Value	Value Type	Length
login_type	String	[0-9]+	String	1:2
orig_url	String		String	1:200
password	String		String	0:350
rds_sso	String	[a-z]**	String	0:4
repository	String	[^/\\*'" ]**	String	0:50
resource_id	String	[0-9a-z]+	String	0:32

Copy Paste Add Remove

To allow access to the ChangePIN application

- Select the required Trunk
- Under Applications select Add
- Click the Web Applications Radio App and Generic Web App then Next
- Enter Application name ChangePIN and Application Type: pinsafe then Next
- Enter the ChangePIN IP address, and under path the location of the ChangePIN install (normally changepin), set the port to 8443, then Next
- Select Next
- Check details are correct, specifically https://<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.

## Verifying the Installation

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 Swivel server.

UAG Login Page

SMS ☒

Turing ☐

### Log On

User name:

192.168.0.165 Password:

PINsafe Password:

Language:

Log On

**Please enter your username in order to continue.**

This site is intended for authorized users only.  
If you experience access problems contact the [site administrator](#).

# Application and Network Access Portal

SMS ☒

Turing ☐

Log On

User name:

graham

AD Server Password:

••••••••

PINsafe Password:

••••

Log On

**Please enter your username in order to continue.**

This site is intended for authorized users only.  
If you experience access problems contact the [site administrator](#).

© 2010 Microsoft Corporation. All rights reserved. [Terms of Use](#).

UAG login using Turing Single Channel Image

# Application and Network Access Portal

SMS ☐

Turing ☒

Log On

User name:

graham

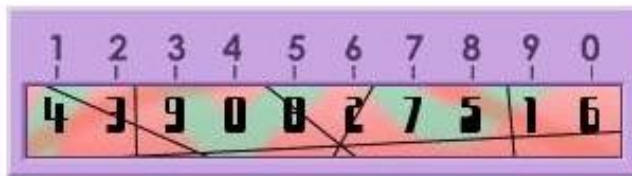
AD Server Password:

.....

PINsafe Password:

....

Log On



This site is intended for authorized users only.  
If you experience access problems contact the [site administrator](#).

© 2010 Microsoft Corporation. All rights reserved. [Terms of Use](#).

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 Swivel server logs and system event logs for any errors or lack of communication as well as the UAG logs. Attempt a login and if required the TURING image, to generate an event then view it under Admin/Web Monitor/Event Viewer/Security. Check the ISA server logs.

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

If the changes made in the UAG are not reflected in the login page, allow sufficient time for the rules to be written on the TMG (wait 10 minutes).

**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**

URL blocking by the UAG. Check that the image can be rendered and that the URL rewriting rules are correct

**The URL /internalsite/images/customupdate/images\*.asp contains an illegal path. The rule applied is Default rule. The method is GET.**

When the message *The rule applied is Default rule* is seen, it means that no rule has been matched and by default the URL is blocked. In the above example the path is incorrect to images.asp.

## Http 500 error

If you get an http 500 error when using xml based integration you may need to edit the token.inc file so that

```
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
```

is replaced with



```
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5.1")
```

Ensure that the UAG can resolve the Swivel server name when hostname is used for connecting by RADIUS. Try with the IP address of the Swivel server.

## Additional Configuration Options

### RADIUS Challenge and Response

The UAG and Swivel supports the use of Challenge and Response authentication.

On the Swivel Administration Console ensure two-stage authentication is set to "Yes" for the RADIUS NAS definition. Secondly, under Server -> Dual Channel, ensure On demand authentication is set to "Yes".

In order to use two-stage authentication on Swivel, all users have to have a password defined. There are two ways to manage this: either set a password for each user under user administration, or enable the option to check password with repository (under Policy -> Password), in which case Swivel uses the AD password. Either way, you need to enter the password for Swivel as well as the AD password. (It might be possible, using the repository password option, to have a custom page that copies the AD password to the Swivel password, but this has not been tested).

If the Swivel password is entered correctly, you will be sent a security string, and a second login page will be displayed, to enter your one-time code.

### PINpad Integration

PINpad integration can be accomplished using [these files](#), and a slight modification to the installation procedure. Please note that this zip file reflects the relative locations of the 3 files included, starting from "InternalSite". The login page goes into /InternalSite/customupdate and the other two into /InternalSite/images/customupdate.

Please ensure that you have Pinpad enabled on your Swivel virtual or hardware appliance, following the instructions [here](#).

Use pinpad.asp instead of images.asp from the original integration, and edit this in a similar way, replacing the internal URL for the Swivel appliance. Keep everything from "/proxy/SCPinPad" as it is. You will also need to make a similar change to StartSession.asp. One important difference to recognise with this solution is that it makes a session start request explicitly. Therefore, you cannot use the /proxy application. Instead, you must use port 8080 and context /pinsafe on a virtual or hardware appliance. This also means that you must have PINsafe version 3.9.2 or later, since earlier versions do not support PINpad natively. Make sure that the firewall rule is configured appropriately. If you have an earlier version of PINsafe, either upgrade, or use [this](#) older solution. If you use the older solution, note the differences below, and ignore any references to StartSession.asp.

Use /customupdate/loginpinpad.asp as the login page.

When configuring the URL rewriting rules, you will need to include pinpad.asp and StartSession.asp in /images/CustomUpdate as accepted pages, unless you have allowed all pages in /images/CustomUpdate. Either set "ignore" for all parameters for these pages, or else permit the following parameters:

- pinpad.asp:
  - ◆ sessionid (or username for the old solution)
  - ◆ padno
- StartSession.asp
  - ◆ username
  - ◆ random

NOTE: this login page assumes that PINsafe is the primary authentication. If it is the secondary, you need to edit the login page (loginpinpad.asp) and change the following line

```
var PINSAFE_PASSWORD_INDEX = 0;
```

to this:

```
var PINSAFE_PASSWORD_INDEX = 1;
```

### ChangePINpad Integration

When publishing access to ChangePINpad, ensure that you enable the following paths during creation:

**Application Properties (pinsafe)**

Endpoint Policy Settings

Web Server Security | Cookie Encryption

Download/Upload | Portal Link | Authorization

General | Web Servers | Web Settings | Authentication

Address type: ☒ IP/Host ☐ Subnet ☐ Regular expression

Addresses:

Paths:

/changePIN  
/proxy

HTTP ports:

HTTPS ports: 8443

☐ Add the default port to the host

Help OK Cancel

This should in turn create the following rules:

		pinsafe_Rule1	Accept	/changePIN(/.* \$)	Ignore	POST, GET
		pinsafe_Rule1_Proxy	Accept	/proxy(/.* \$)	Ignore	POST, GET

Beware that if you add paths to the published application afterwards, the rules for these paths will not be created. So ensure that you enter the paths at creation time.

## Button size and aspect ratio

The Button size and aspect ratio is controlled by the settings in the login page:

```
document.all.otp.innerHTML = ''; }
```

change the height and width settings to the value that is appropriate.

## XML Authentication

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

XML authentication has not been tested with the current version of UAG and is supplied for reference if required, RADIUS authentication is the preferred method of authentication.

Note that when using a Swivel virtual or hardware 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 Swivel virtual or hardware appliance versions.

This step is not required when RADIUS authentication is used. RADIUS authentication is the preferred method of authentication. To enable the token.inc file, create a repository of type ?Other? on the UAG 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).

#### Configure a Swivel Agent (For XML Authentication)

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

The screenshot shows the 'Agents' configuration page in the Swivel Administration Console. It contains two agent configuration forms. The first agent is named 'local' with a hostname/IP of '127.0.0.1'. The second agent is named 'IIS' with a hostname/IP of '192.168.1.1'. Both agents have a shared secret (represented by dots), a group set to '---ANY---', and authentication modes set to 'ALL'. Each agent configuration has a 'Delete' button next to it.

To create the repository, do the following-

1. Access the UAG 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

Edit the file Token.inc with the required shared secret and to represent the Swivel server IP address and Swivel install name, Note for all Swivel installs this needs to point to the PINsafe server on port 8080 and not the proxy port 8443.

```
m_secret = "secret"

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

**Note** If you get an http 500 error when using xml based integration you may need to edit the token.inc file so that

```
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
```

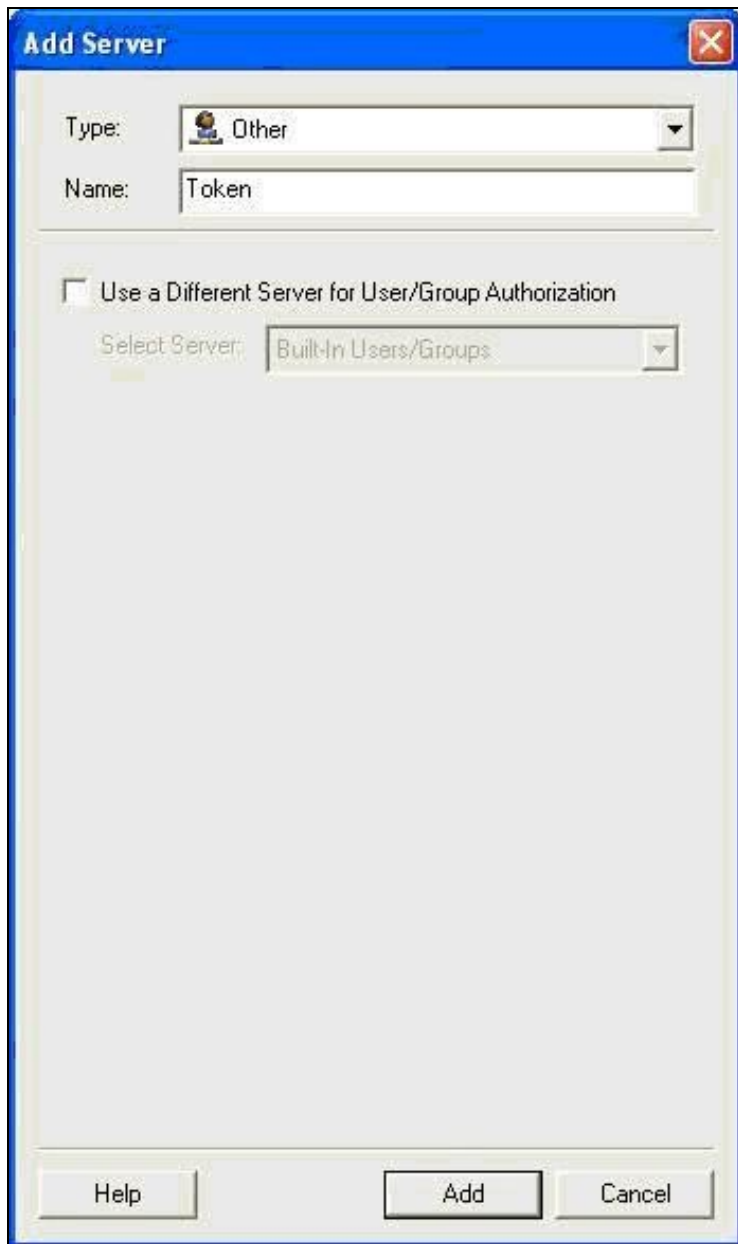
is replaced with

```
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5.1")
```

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"
```



A screenshot of a Windows-style dialog box titled "Add Server". The dialog has a blue title bar with a close button (X) in the top right corner. Inside, there are two input fields: "Type:" with a dropdown menu showing "Other" and a small icon, and "Name:" with a text box containing "Token". Below these is a checkbox labeled "Use a Different Server for User/Group Authorization", which is currently unchecked. Under the checkbox is a "Select Server:" dropdown menu showing "Built-In Users/Groups". At the bottom of the dialog are three buttons: "Help", "Add", and "Cancel".

**Add Server**

Type: Other

Name: Token

☐ Use a Different Server for User/Group Authorization

Select Server: Built-In Users/Groups

Help Add Cancel

## Known Issues and Limitations

If upgrading the UAG to a higher service pack, 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.

Upgrading from RTM Update 2, to SP1 will cause the InternalSite rules, on the UAG to be removed, or changed back to defaults.

If the login page is viewed incorrectly as a mobile page then this [workaround](#) will allow the correct page to be displayed, and works with Windows 7 and Windows 8.

## Additional Information

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