

Table of Contents

1 Microsoft IAG Integration.....	1
1.1 Introduction.....	1
1.2 Prerequisites.....	1
1.3 Baseline.....	1
1.4 Architecture.....	1
1.5 Installation.....	1
1.6 Verifying the Installation.....	1
1.7 Uninstalling the PINsafe Integration.....	1
1.8 Troubleshooting.....	1
1.9 Known Issues and Limitations.....	1
1.10 Additional Information.....	1
2 Microsoft IAG Multiple Authentication.....	2
2.1 PINsafe and IAG/UAG Integration using multiple repositories.....	2
2.2 Approach.....	2
2.3 Implementation.....	2
2.4 User Experience.....	4
3 Microsoft IAG SMS login video.....	7
3.1 Microsoft IAG SMS login Video.....	7
4 Microsoft IAG Turing login video.....	8
4.1 Microsoft IAG TURing login Video.....	8

1 Microsoft IAG Integration

1.1 Introduction

This document covers the integration of PINsafe with the Microsoft Intelligent Application Gateway.

1.2 Prerequisites

PINsafe 3.x

Microsoft IAG

The IAG integration guide can be found here: [IAG SP1 Integration Guide](#) and here [SP2 Integration Guide](#)

1.3 Baseline

1.4 Architecture

1.5 Installation

1.5.1 PINsafe Integration Configuration

1.5.2 Access Device or Application Integration

1.5.3 Additional Installation Options

1.6 Verifying the Installation

1.7 Uninstalling the PINsafe Integration

1.8 Troubleshooting

1.9 Known Issues and Limitations

1.10 Additional Information

2 Microsoft IAG Multiple Authentication

2.1 PINsafe and IAG/UAG Integration using multiple repositories

This article explains how to use PINsafe with Microsoft IAG/UAG so that different applications are available to users depending on how they authenticated.

These notes are based on IAG Version 3.7 and PINsafe Version 3.6

This article shows the approach required to add this functionality to a standard IAG/UAG and PINsafe integration. Standard integration notes are available from the [Microsoft IAG Integration](#) guide and should also be referred to.

2.2 Approach

The approach is to create two different repositories on the IAG. One repository will use Agent-XML for authentication the other will use RADIUS.

One repository will be associated with single channel authentication, the other with dual channel authentication.

The login page will determine which repository the user is authenticating based on whether the user has requested a single channel ([TURing](#)) image or not.

The IAG will be configured to allow access to specific applications based on the repository a user has authenticated to.

On the PINsafe server the NAS or Agent associated with the IAG Dual channel repository will be set to accept dual channel authentication only.

2.3 Implementation

The names used for repositories etc are just examples, but sometimes names are important, eg the repository of type "other" needs to have the same name as the associated .inc file and needs to be reflected in the checkradio() function in PinsafeLogin.asp

2.3.1 PINsafe Configuration

In this example radius will be used for dual channel authentications only so on the PINsafe server

Enable RADIUS server

Create a NAS entry for the IAG

Set ip address and shared secret as required

Set mode to dual channel only for the NAS

Create an Agent entry for the IAG

Set ip address and shared secret as required

2.3.2 IAG Repository Configuration

Copy images.asp to von\InternalSite\Images\CustomUpdate

Ensure that it is the version that can also handle index images and ensure that the IP addresses etc match the PINsafe server

```
if request.querystring("index") <> "" then
    Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
    objWinHttp.Open "GET", "http://127.0.0.1:8080/pinsafe/DCIndexImage?username=" & request.querystring("username"), false
else
    Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
    objWinHttp.Open "GET", "http://127.0.0.1:8080/pinsafe/SCImage?username=" & request.querystring("username"), false
end if
```

Create a new Repository called pinsafe of type other.

Copy the pinsafe.inc file to von\InternalSite\inc\CustomUpdate

Edit pinsafe.inc so that the secret (m_secret), ip address and port matches that of the PINsafe server

```
function checkswivelpwd (userName, password)
LIGHT_TRACE "checkswivelpwd entered for " & userName
LIGHT_TRACE "SWIVEL - lets check if the password is right"
Dim strHTML
m_secret = "secret"
Dim objWinHttp
m_request = "<?xml version=""1.0"" ?><SASRequest><Version>1.0</Version><Action>login</Action><Username>" & username & "</Username><OTC>" & password & m_secret & "</Secret></SASRequest>"
Set objWinHttp = Server.CreateObject("WinHttp.WinHttpRequest.5")
objWinHttp.Open "GET", "http://<ipaddress>:8080/pinsafe/AgentXML?xml=" & m_request, false
```

Create a new Repository called pinsaferadius or type RADIUS.

Enter the details of the PINsafe RADIUS server on the config screen.

2.3.3 Trunk Configuration

For the trunk you are using eg portal, ensure that both pinsafe and pinsaferadius repositories are associated with the page

Also ensure that the option User Selects from A List of Servers is set

Set the login pages to be PINsafeLogin.jsp

The screenshot shows the 'Advanced Trunk Configuration [portal]' window with the 'Authentication' tab selected. The 'Authenticate User on Session Login' section is checked. Under 'Select Authentication Servers', a list contains 'pinsaferadius' and 'pinsafe', with 'pinsafe' selected. To the right of the list are 'Add...' and 'Remove' buttons, and up/down arrow buttons. Below the list, the 'User Selects From a List of Servers' radio button is selected. Under this, 'Show Server Names' is checked. The 'User Must Provide Credentials for Each Selected Server' radio button is unselected, and 'Use the Same User Name' is checked. The 'Use Integrated Windows authentication' radio button is unselected, and both 'Enable NTLM protocol' and 'Enable Kerberos protocol' are checked. 'Enable Users to Add Credentials On-the-Fly' and 'Enable Users to Change Their Passwords' are checked. Under 'Enable Users to Change Their Passwords', 'Notify User' is unchecked and the value '7' is entered in the 'Days Prior to Expiration' field. 'Enable Users to Manage Their Credentials' and 'Enable Users to Select Language' are checked. 'Skip client compliance checks when accessing a SharePoint site outside of a session' is unchecked. At the bottom, 'Login Page:' and 'On-the-Fly Login Page:' both point to 'PinsafeLogin.asp'. 'Permitted Authentication Attempts:' is set to '3'. 'Block Period:' is set to '0' minutes.

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:

pinsaferadius	
pinsafe	

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

Now copy the PINsafeLogin.jsp to von\InternalSite

Edit the PINsafeLogin.jsp to ensure that the repository names match those that you are using and that the dual channel and single channel authentication are matched to the correct repository.

```
function checkradio()
{
    var radiovalue = eval(document.form1.swivel[1].checked);
    var r = document.getElementById("repository");
    if (radiovalue == true)
    {
        //alert("turing");
        //TURING selected, therefore refresh TURING image
        updateotp();
        //repository for TURING is pinsafe
        r.value = "pinsafe"
    } else{
        //alert("sms");
        updateindex(); //if we are using multi-sms update index will display required index
        r.value = "pinsaferadius"
        //repository for TURING is pinsaferadius
    }
}
```

With different repositories aligned to different authentication methods, it is possible then to make some applications only accessible when a user has authenticated using the dual channel method.

[illegible]

The user is presented with the option of authenticating via SMS or TURING.

To authenticate the user enters their username and then clicks on the authentication method they wish to use.

If they select TURING and TURING image is displayed.

Web site

Please provide the following:

SMS ☐

Turing ☒

User Name:

Password:

Language:



If they select SMS (and multi-SMS is being used) the index of the security string that they need to use is displayed.

Web site

Please provide the following:

SMS ☒

Turing ☐

User Name:

Password:

Language:

English (default) ▼

00

(If they have no valid SMS strings, -1 is shown)

When they make their selection the login page automatically associates them with the correct repository.

After authentication they will only have access to applications appropriate to their method of authentication.

3 Microsoft IAG SMS login video

3.1 Microsoft IAG SMS login Video

[PINsafe_IAG_SMS_login.swf](#)

4 Microsoft IAG Turing login video

4.1 Microsoft IAG TURING login Video

[PINsafe_IAG_Turing_login.swf?](#)