Citrix Access Gateway Advanced Edition Installation Notes

Created November 2006 Graham Field
Updated October 2007 Graham Field
Updated May 2008 Chris Russell

Table of Contents

Introduction

This configuration document outlines how to integrate PINsafe with Citrix Access Gateway Advanced Edition using Active Directory authentication in addition to the PINsafe authentication.

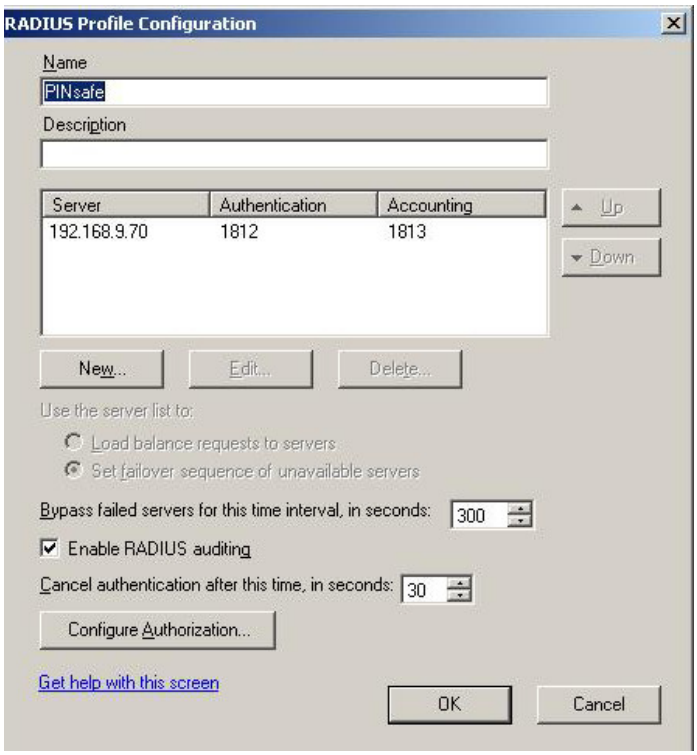
Prerequisites

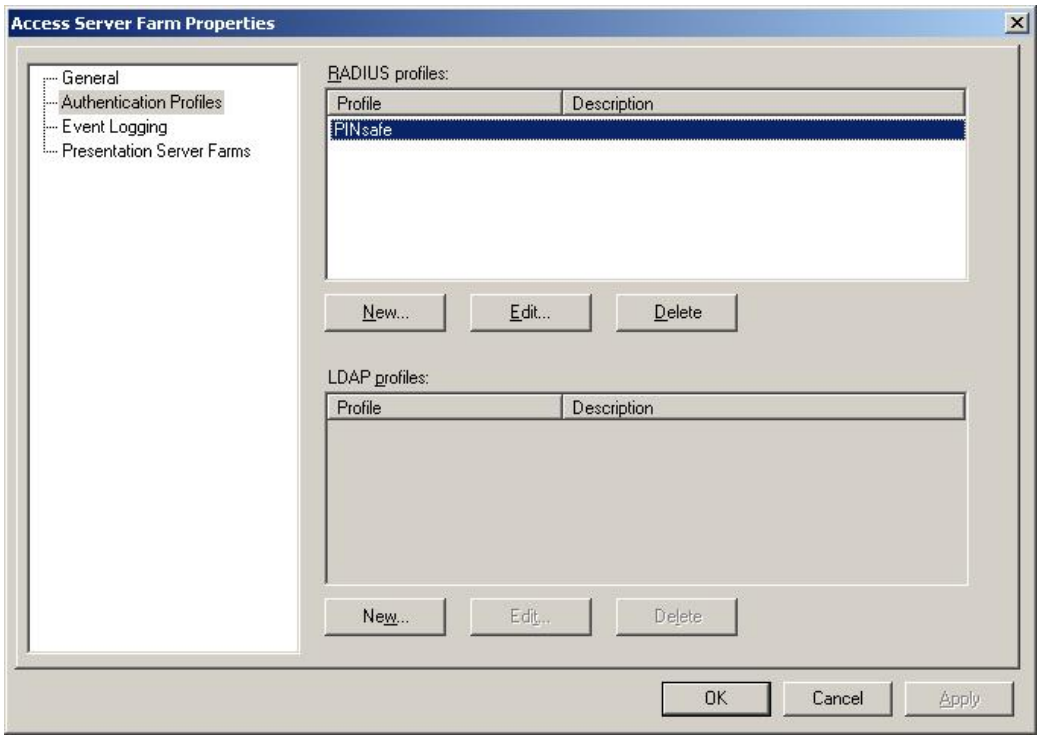
Citrix Access Gateway 4.5
Citrix Advanced Access Control 4.5
Citrix Access Management Console 3.0 with configured login points
Correct Citrix Licensing
PINsafe server
For Single Channel the PINsafe server IP needs to be reachable for authentication (i.e. this means an external IP address or a NAT for the PINsafe server IP

Installation

Configure the RADIUS server

Right Click on the Access Gateway server farm and select Edit Farm Properties. Select the Authentication Profiles and for RADIUS profiles click on New. Enter a name and description for the server and then click on New. In the RADIUS server configuration enter the PINsafe server IP address, modify the Authentication and Accounting ports as required then click on OK.





Modify the logon page

Skip this step if Single Channel authentication is not required
Locate the Logon page and then edit the Login.ascx
Example C:\Inetpub\wwwroot\CitrixLogonPoint\External
The following line needs to be edited to be the IP address of the PINsafe server, and if required to use https (normally on port 8443)

var sUrl="http://192.168.9.70:8080/pinsafe/SCImage?username=";

If you are using a PINsafe appliance the url may need to reflect the use of the image proxy; therefore it would be of the form

var sUrl="https://192.168.9.70:8443/proxySCImage?username=";

The position of the displayed Turing button and Security String can also be modified by editing the following lines:

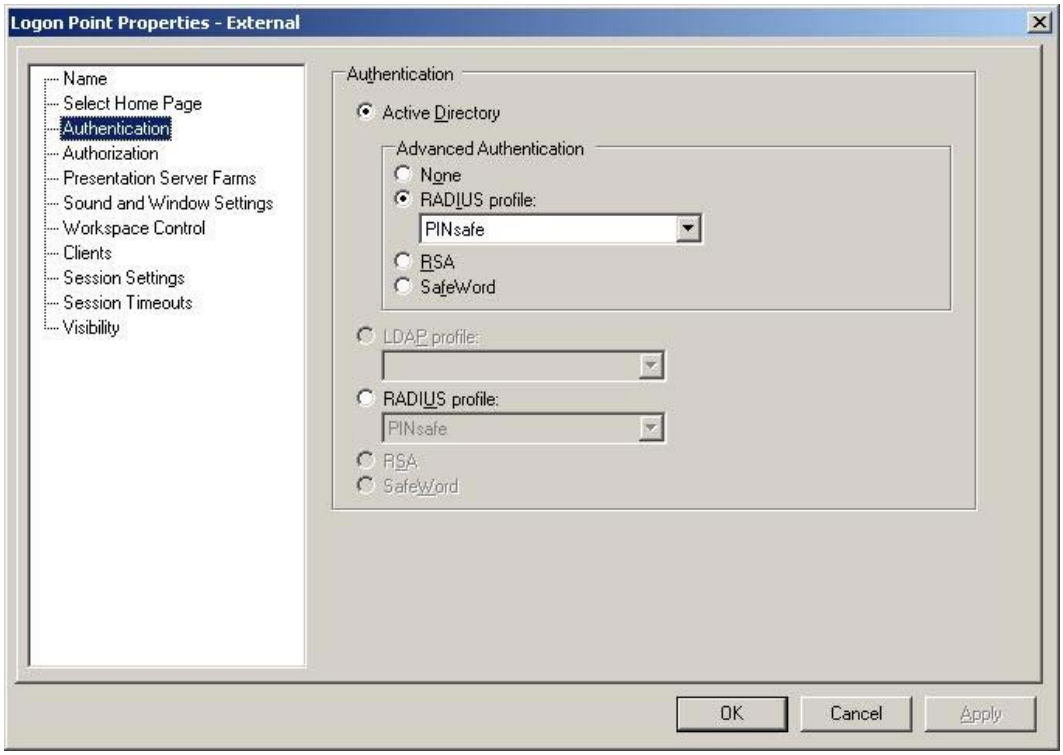
```
document.write("<input type=button name=btnTuring value=Turing
onclick=ShowTuring() class='submitbutton' styleHIDDEN='visibility:hidden;
position: absolute; left:250;top:302;width:75;'>");

document.write("<img id=imgTuring name=imgTuring
style='visibility:hidden;position: absolute; left:100;top:350;'>");
```

where the values of left and top can be altered.

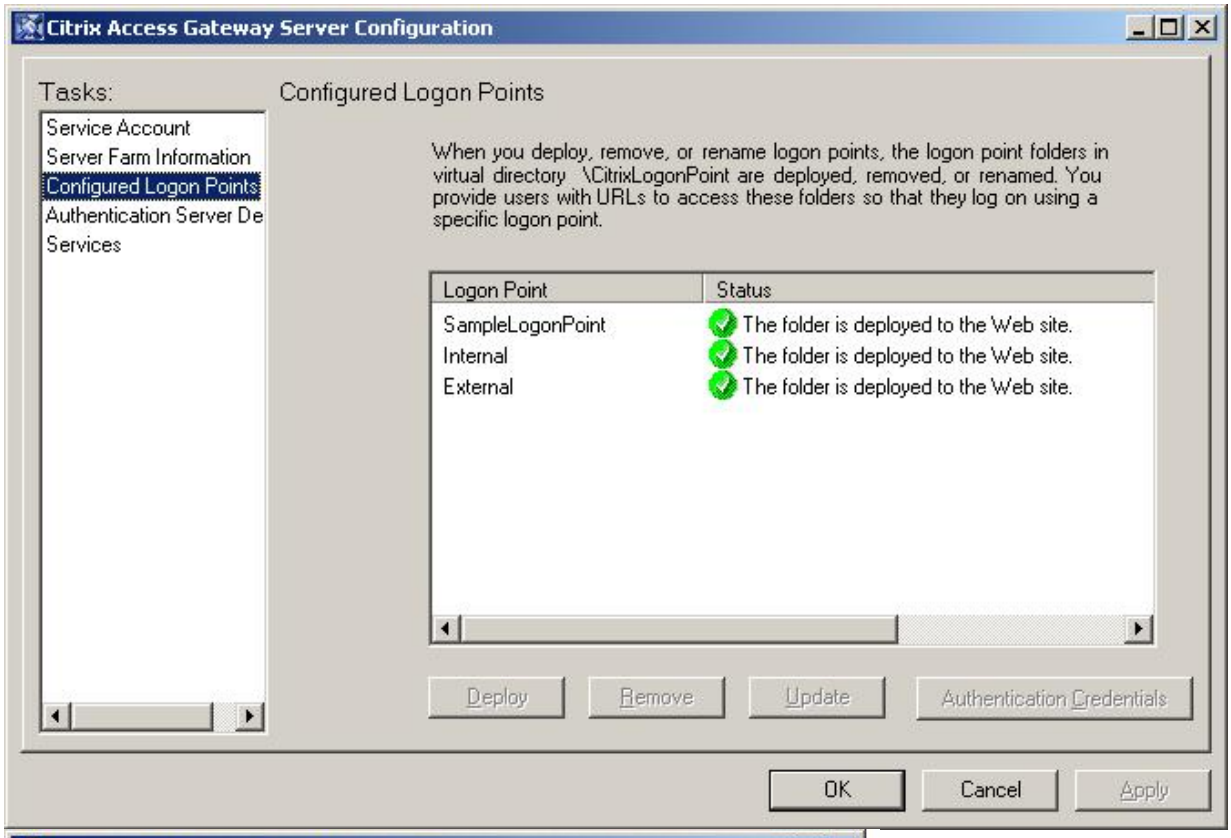
Configure the logon page to use PINsafe

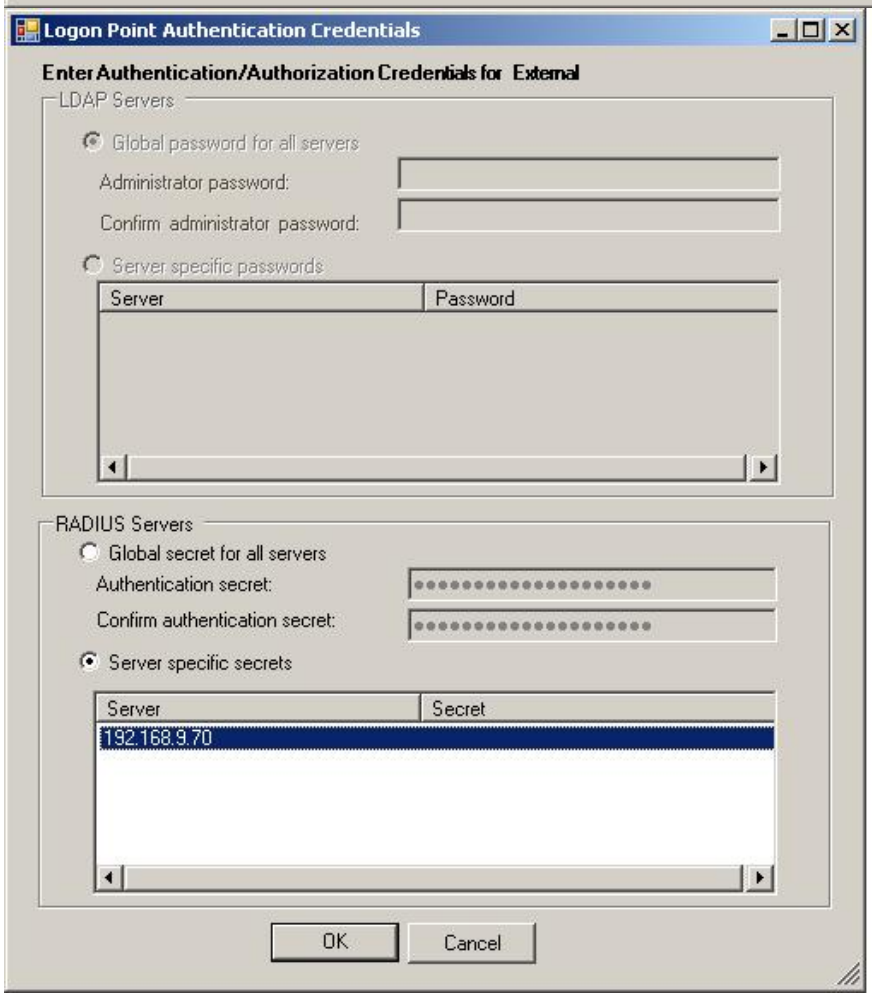
Right click on the selected Logon Point and select Edit logon point.Select Authentication and ensure that the Active Directory Radio button is selected. Under Advanced Authentication select the RADIUS profile radio button and from the drop down menu select the PINsafe RADIUS server.
Under Authorization ensure that Group Authorization is set to Active Directory. Ensure that 'Authentication and group authority use the same password' is not selected.
Under Session Settings ensure that users have access to the Active Directory domain where their usernames and passwords are held, and this should be the same domain that PINsafe is using to read its usernames.



Configure RADIUS server authentication

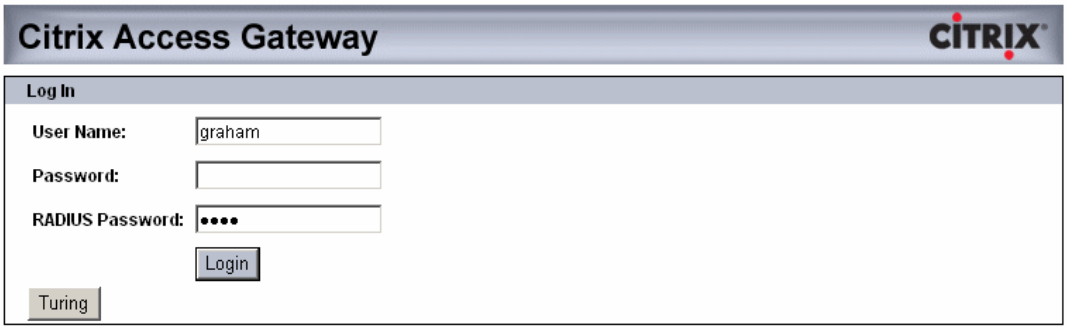
This is configured from the Citrix Access Gateway Server Configuration. Select the Configured Logon Points and then click on the Logon Point required for PINsafe access, then click on the Authentication Credentials. RADIUS authentication can be configured by using either a Global secret or server specific secret, this needs to be the same as the shared secret on the PINsafe server. When complete select deploy to update the Citrix Access Gateway.


Citrix Access Gateway Server Configuration
Tasks:
Service Account
Server Farm Information
Configured Logon Points
Authentication Server De
Services
Configured Logon Points
When you deploy, remove, or rename logon points, the logon point folders in virtual directory \CitrixLogonPoint are deployed, removed, or renamed. You provide users with URLs to access these folders so that they log on using a specific logon point.
Logon Point
Status
SampleLogonPoint
The folder is deployed to the Web site.
Internal
The folder is deployed to the Web site.
External
The folder is deployed to the Web site.
Deploy
Remove
Update
Authentication Credentials
OK
Cancel
Apply

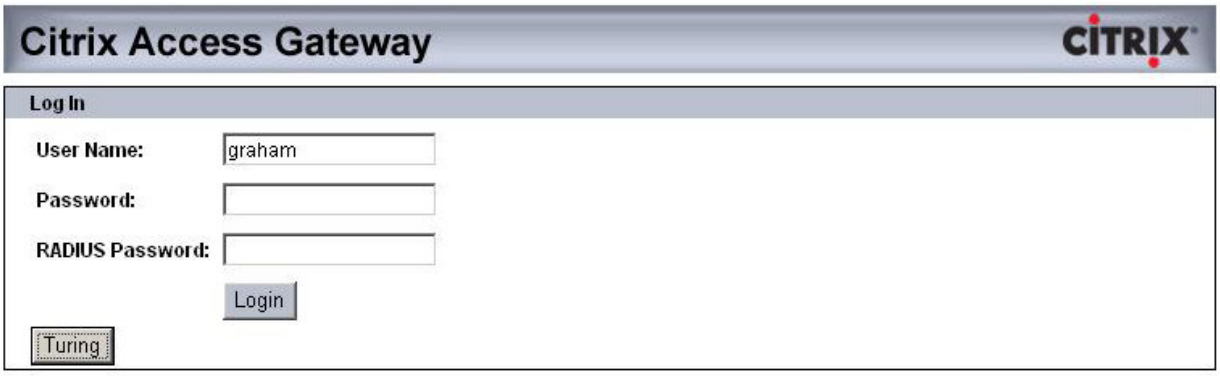

Logon Point Authentication Credentials
Enter Authentication/Authorization Credentials for External
LDAP Servers
Global password for all servers
Administrator password:
Confirm administrator password:
Server specific passwords
Server
Password
RADIUS Servers
Global secret for all servers
Authentication secret:
Confirm authentication secret:
Server specific secrets
Server
Secret
192.168.9.70
OK
Cancel

Testing

In a web browser load the logon page. The Single and Dual Channel should both function as required. For Dual channel enter the User Name, AD password, and the One Time Code in the RADIUS password field.



For Single Channel enter the User Name, AD password, then click on the Turing button to generate a single channel login image. Carry out a PIN extraction and enter the One Time Code in the RADIUS password field.



Troubleshooting

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

Additional Information

For assistance in the PINsafe installation and configuration please contact your reseller or email Swivel Secure support at support@swivelsecure.com