Table of Contents

Table of Contents

1 Citrix Access Gateway 5 VPX

1.1 Introduction

Please refer to the documentation located at:

Citrix Access Gateway Standard 5.x

2 Citrix Access Gateway Access Controller 5.0

PINsafe integrates with the Access Controller 5.0 using RADIUS authentication. The following authentication methods are supported:

- SMS
- Mobile Phone Client
- Email
- Taskbar utility

Please refer to the Citrix Access Controller Administration guide for further information on configuring the Access Controller.

The single Channel graphical TURing image cannot currently be embedded into the login page when using the Access Controller 5.0, but we hope to offer this enhancement at a future date. Please contact Swivel Secure to register your interest.

3 Citrix Access Gateway Advanced 4.x

4 Introduction

This document covers the integration of Citrix Access Gateway Advanced edition 4.x.

5 Prerequisites

PINsafe 3.x

The CAG 4.5 integration guide is available here: Citrix Access Gateway Advanced edition 4.5

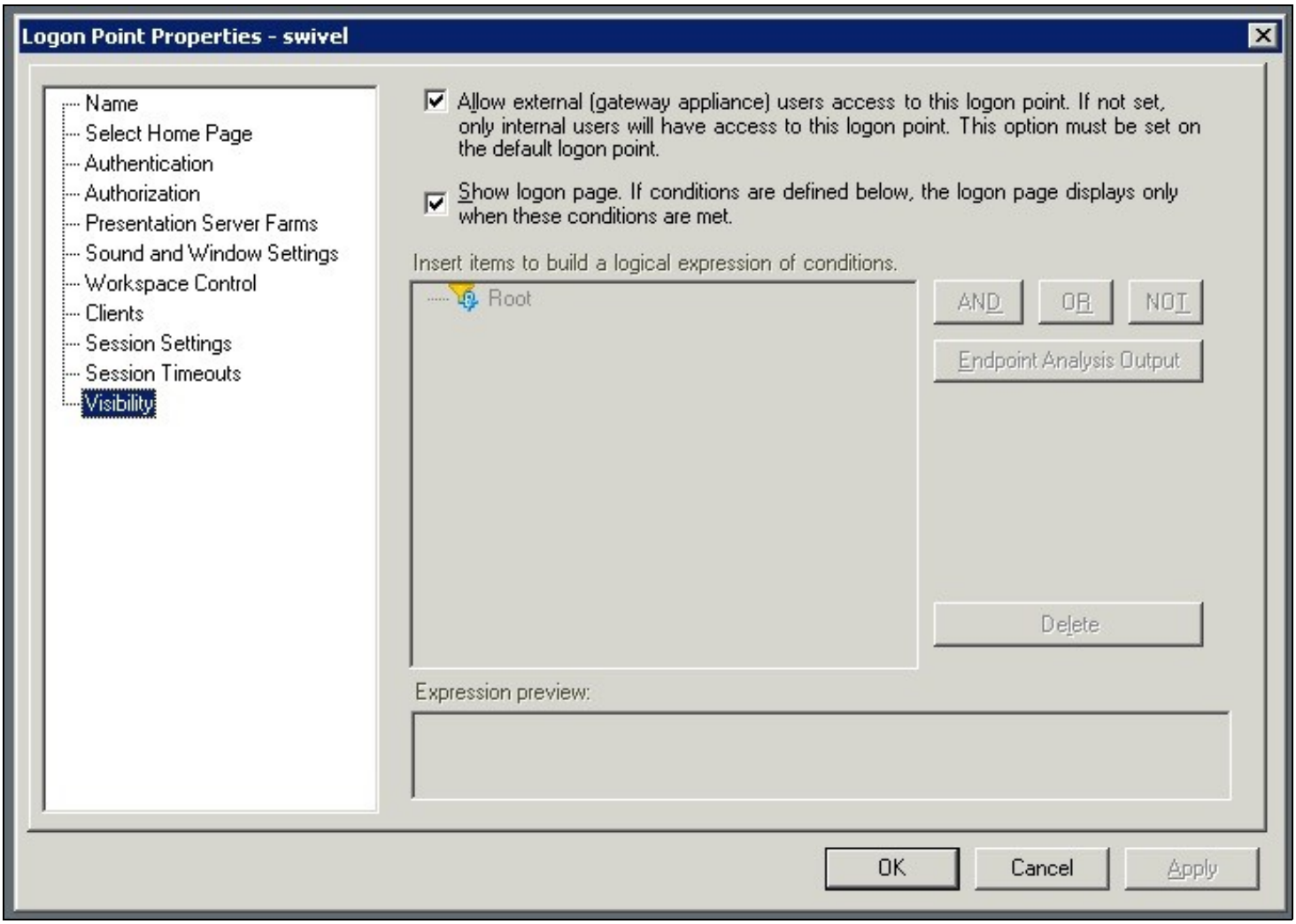
The CAG 4.5.8 integration guide is available here: Citrix Access Gateway Advanced edition 4.5.8

Note: For PINsafe Single Channel authentication the PINsafe server IP needs to be reachable by the client (i.e. this means an external IP address or a NAT for the PINsafe server IP). An SSL certificate is usually installed on the PINsafe server to prevent the browser from displaying errors regarding self signed certificates or sites without SSL certification. Swivel Secure can assist with the deployment of the certificate, but this must be purchased and applied for by the end user or their reseller.

Additional Integration supplementary documentation is provided below

6 Installation

Ensure on the Logon Point Properties, that under Visibility, the check box is ticked for 'Allow external (gateway appliance) users access to this logon point. If not set, only internal users will have access to this logon point. This option must be set on the default logon point.'



7 Additional Installation Options

7.1 Remove automatic TURing image automatically displaying

To prevent the auto-loading, remove (or comment out) the onBlur method on username:

```
//     userField.onblur = ShowTuring;
```

to

```
userField.onblur = ShowTuring;
```

7.2 Prevent browser caching TURing image

To stop image caching, add a random number to the image request **+ "&random=" + Math.round(Math.random()*1000000);**

Example:

```
//Set the image SRC and make it visible
varImg.src = sUrl + sUser + "&random=" + Math.round(Math.random()*1000000);
```

7.3 Prevent the cursor from automatically entering the OTC field

Remove the following line from Login.ascx

```
//Set focus to the OTC input
document.getElementById(sNameOfOTCText).focus();
```

7.4 Change the TURing button text

To change the prompt for Turing, edit the Login.ascx file and look for the line:

```
turingBtn.value = "Turing";
```

and change it to

```
turingBtn.value = "Refresh Image";
```

7.5 Verifying the Installation

7.6 Uninstalling the PINsafe Integration

7.7 Troubleshooting

7.8 Known Issues and Limitations

7.9 Additional Information

8 Citrix Access Gateway Standard 4.x

9 Introduction

This document covers the integration of Swivel with the Citrix Access Gateway Standard edition. The standard edition allows authentication using SMS, Email, Mobile Phone applet, PINsafe Taskbar, but does not allow the single channel image to be embedded into the login page. To allow the single channel image to be embedded into the login page, the Advanced Access Controller is required, see Citrix Access Gateway Advanced 4.x

10 Prerequisites

Swivel 3.x

Citrix Access Gateway 4.x

11 Baseline

12 Architecture

Authentications are made against Swivel using RADIUS.

13 Installation

14 Swivel Configuration

14.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

14.2 Setting up PINsafe Dual Channel Transports

See Transport Configuration

14.3 Citrix Access Gateway Standard Edition Integration

Follow the Citrix Access Gateway Standard Edition Administration guide to configure RADIUS authentication.

15 Additional Information

For additional features use the Advanced Access Controller. This allows customised login pages and the Single Channel Turing Image authentication, see Citrix Access Gateway Advanced 4.x

16 Citrix Access Gateway Standard 5.x

17 Introduction

This document covers the integration of Swivel with the Citrix Access Gateway Standard edition. The standard edition allows authentication using SMS, Email, Mobile Phone applet, Swivel Taskbar, but does not allow the single channel image to be embedded into the login page. To allow the single channel image to be embedded into the login page, the following options are available:

- Advanced Access Controller is required, see Citrix Access Gateway Advanced 4.x
- Proxy the login request to a Web Interface login Citrix Access Gateway Web Interface Proxy

18 Prerequisites

Swivel 3.x

Citrix Access Gateway 5.x

19 Baseline

PINsafe 3.8

CAG Standard 5.0.3

20 Architecture

Authentications are made against Swivel using RADIUS.

21 Installation

22 Swivel Configuration

22.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

22.2 Setting up PINsafe Dual Channel Transports

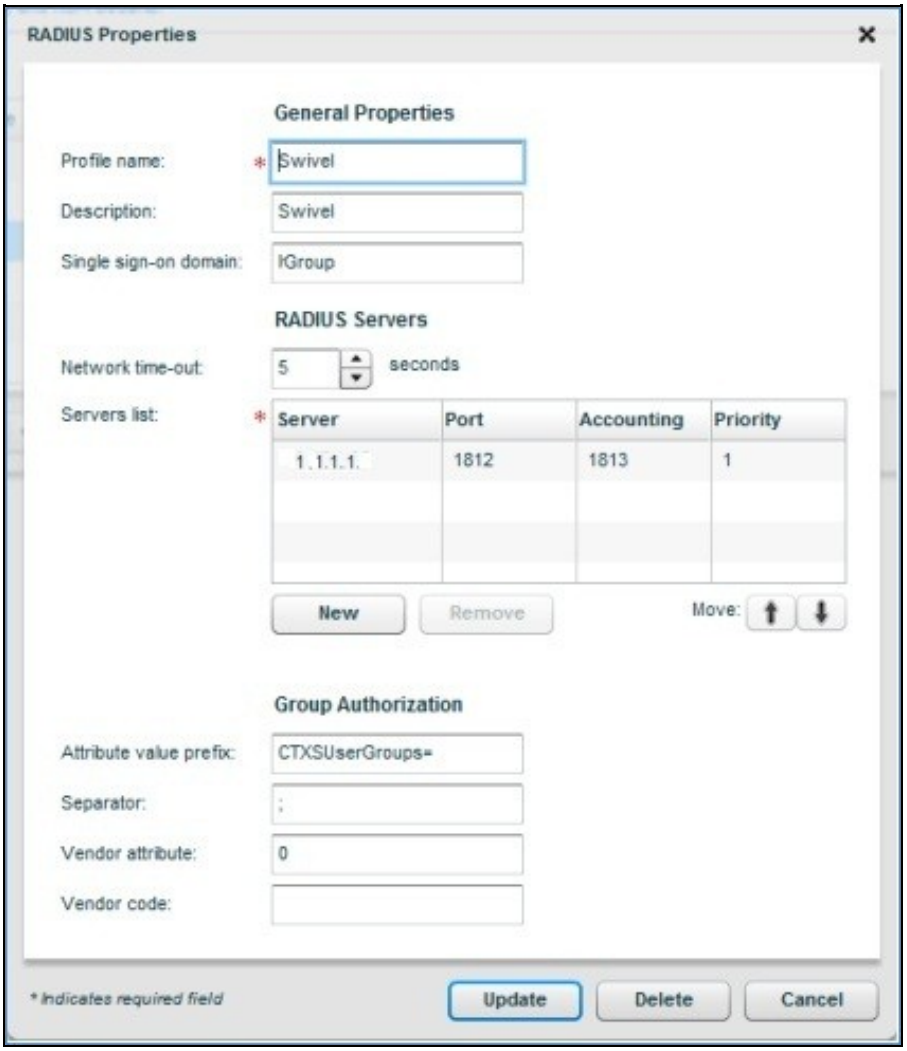
See Transport Configuration

23 Citrix Access Gateway Standard Edition Integration

Follow the Citrix Access Gateway Standard Edition Administration guide to configure RADIUS authentication.

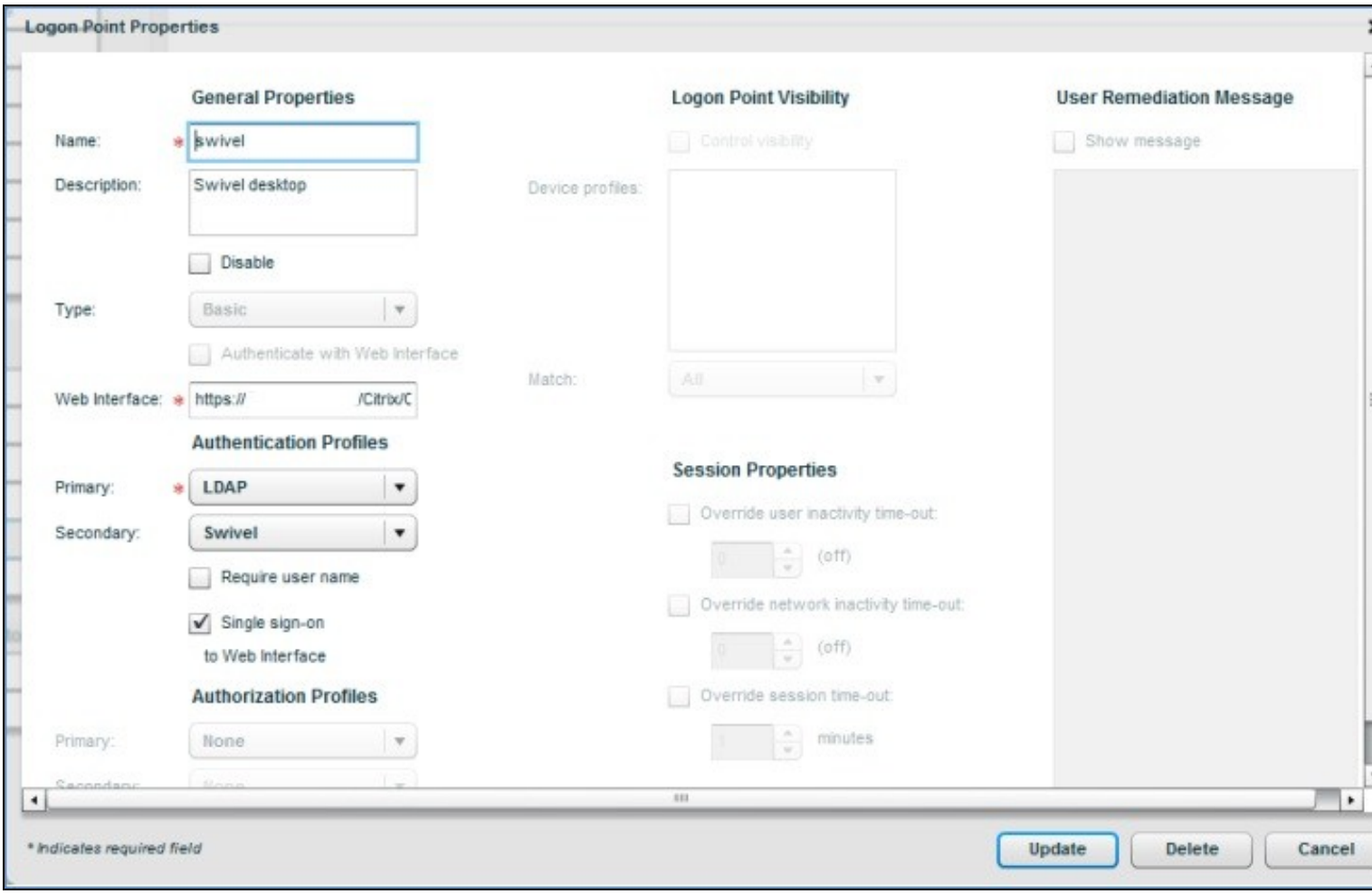
23.1 CAG RADIUS Properties

On the CAG Configuration, configure one or more PINsafe instances as a RADIUS server.



23.2 CAG logon Point Properties

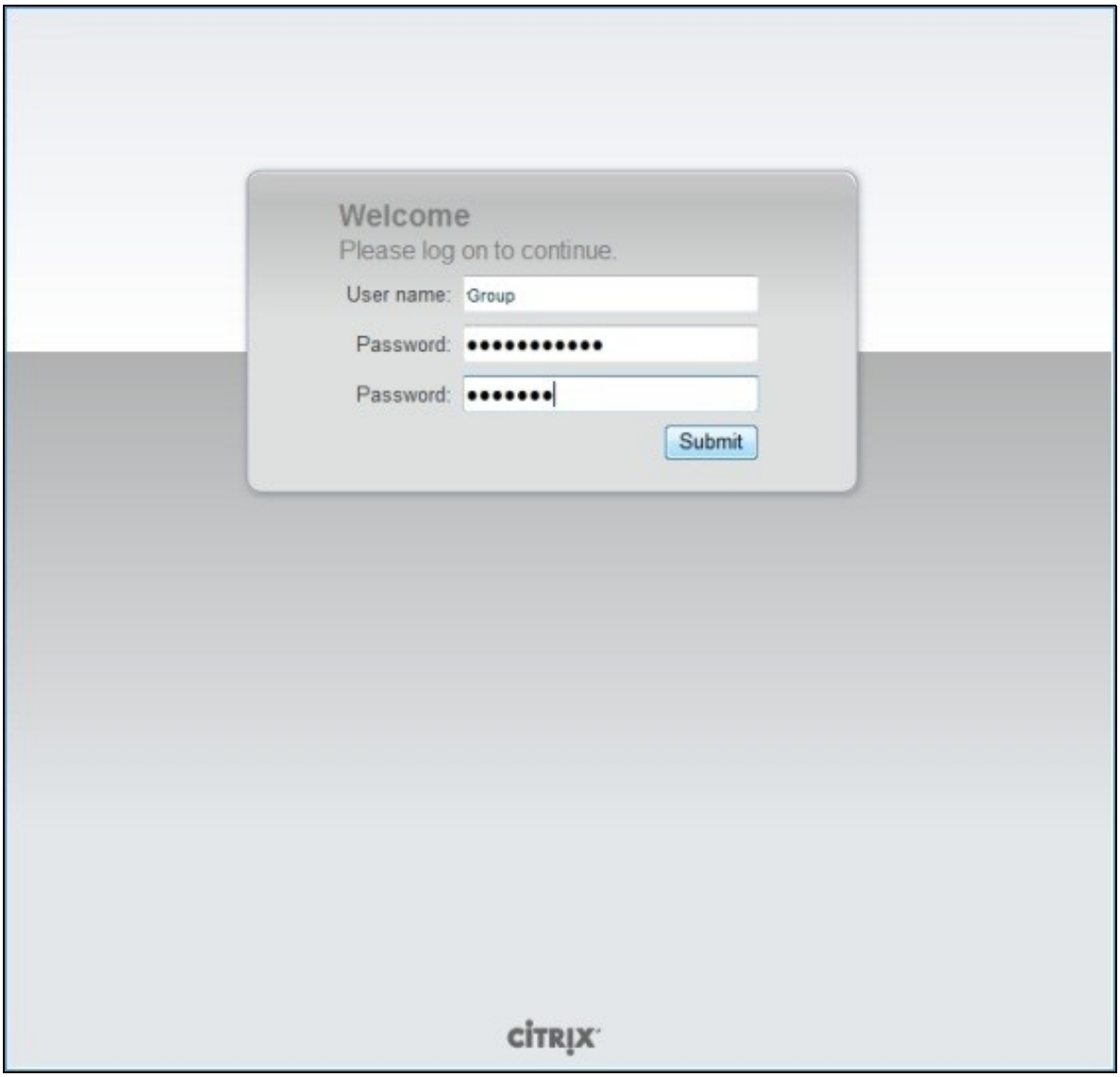
Configure Swivel as an authentication server. Swivel would usually be configured as a secondary authentication server with AD as the primary authentication server using RADIUS. In this example Single Sign ON is being used to the Citrix Web Interface, and has been created as a basic logon point.


Logon Point Properties
General Properties
Name:
swivel
Description:
Swivel desktop
Disable
Type:
Basic
Authenticate with Web Interface
Web Interface:
https://
/Citrix/C
Authentication Profiles
Primary:
LDAP
Secondary:
Swivel
Require user name
Single sign-on
to Web Interface
Authorization Profiles
Primary:
None
Logon Point Visibility
Control visibility
Device profiles:
Match:
All
Session Properties
Override user inactivity time-out:
(off)
Override network inactivity time-out:
(off)
Override session time-out:
minutes
User Remediation Message
Show message
* Indicates required field
Update
Delete
Cancel

24 Additional Installation Options

25 Verifying the Installation

Browse to the CAG login page and enter username, AD Password and OTC from the SMS or Mobile Phone Client. Check the PINsafe logs to ensure that a RADIUS request has been seen.



26 Uninstalling the PINsafe Integration

27 Troubleshooting

28 Known Issues and Limitations

29 Additional Information

For additional features use the Advanced Access Controller. This allows customised login pages and the Single Channel Turing Image authentication, see Citrix Access Gateway Advanced 4.x

30 Citrix Access Gateway Web Interface Proxy

31 Introduction

This document is to supplement the Citrix Access Gateway and Citrix Web Interface documentation for the deployment of PINsafe on the Web Interface and using the Secure Ticket Authority to pass authentication from the Citrix Access Gateway to the Citrix Web Interface.

32 Prerequisites

Citrix Access Gateway 5.x

Citrix Web Interface 5.x

PINsafe 3.x

33 Baseline

Citrix Access Gateway 5.0

Citrix Web Interface 5.4

PINsafe 3.8

34 Architecture

When a user authenticates to the Citrix Access Gateway, the authentication is passed to the Web Interface and the user may use PINsafe authentication.

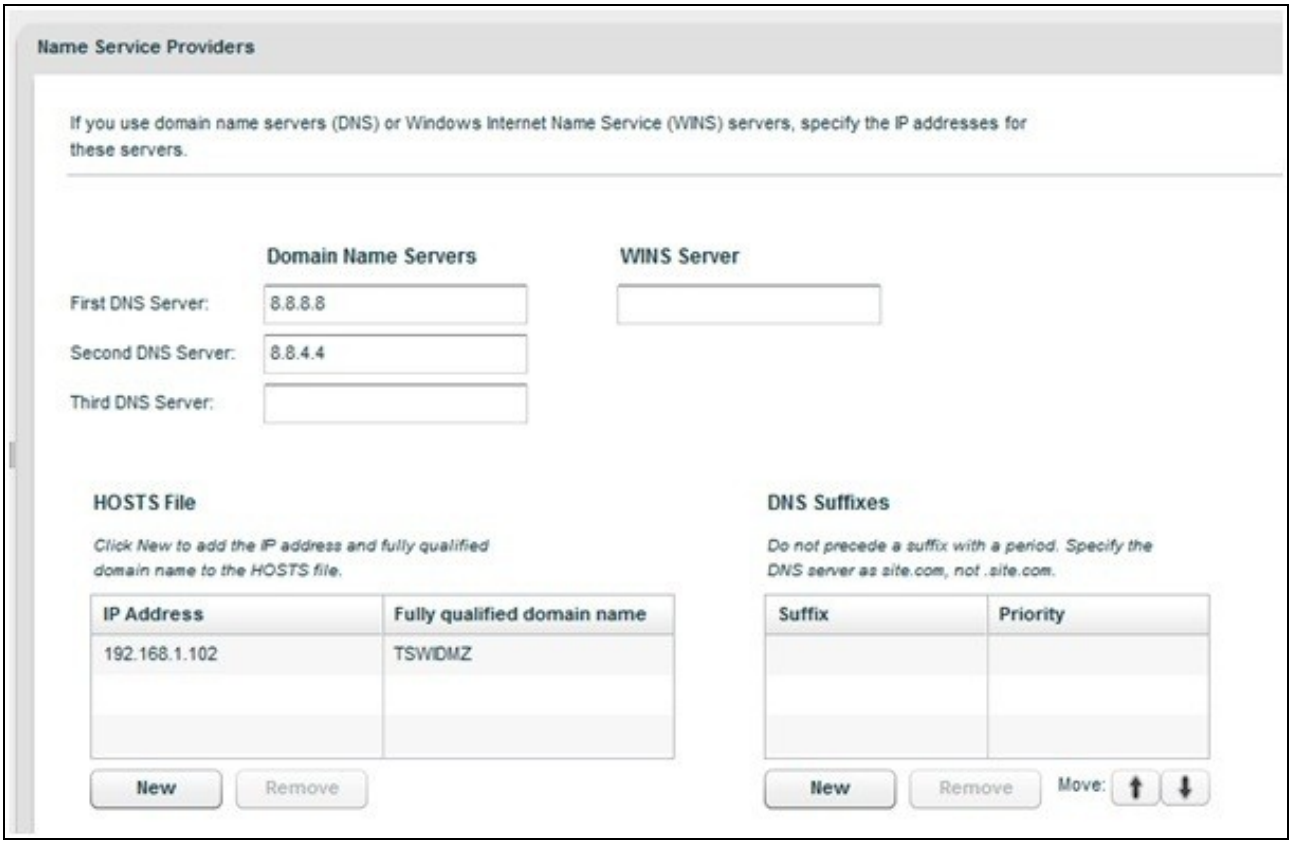
35 Installation

35.1 PINsafe and Web Interface Integration Configuration

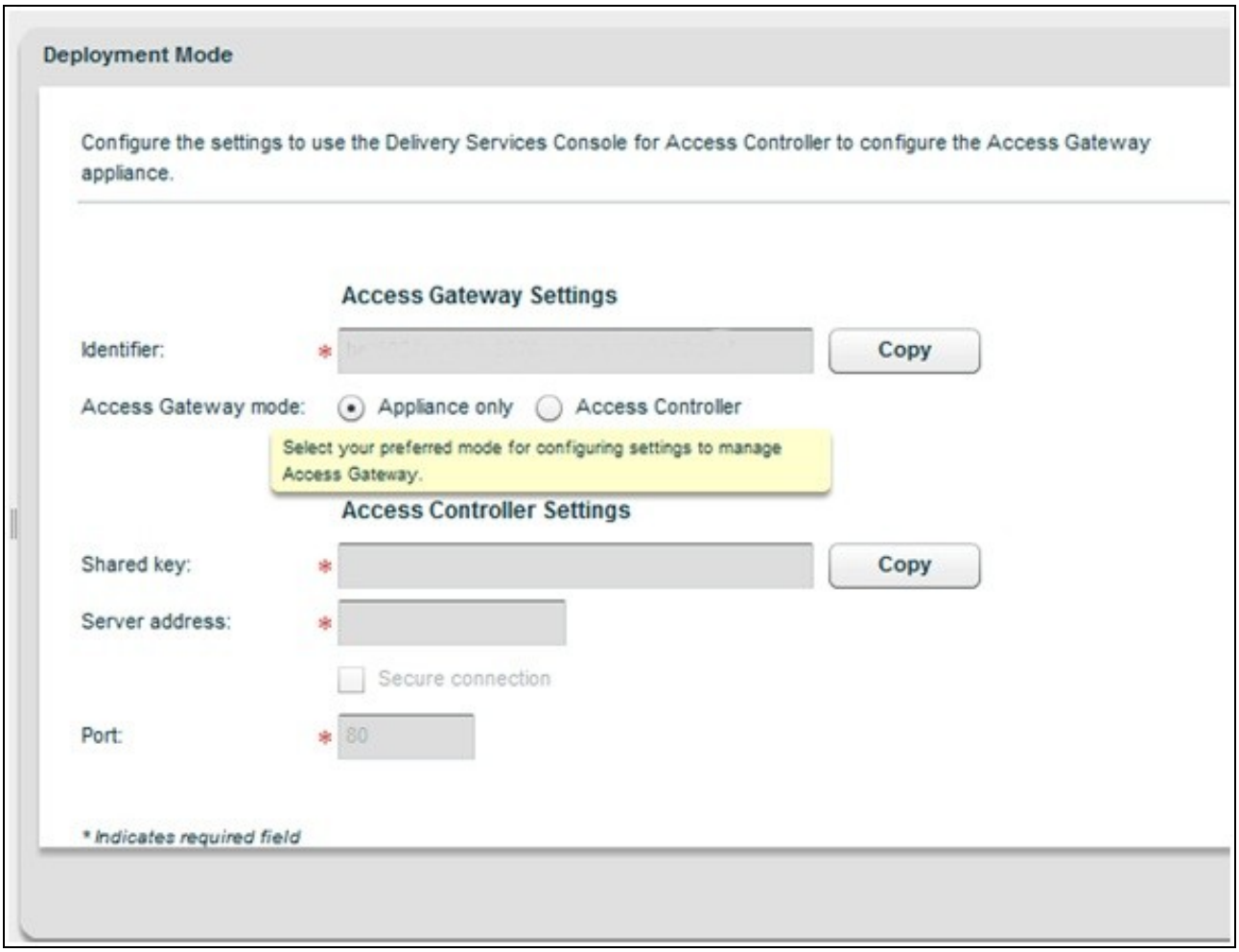
Follow the steps for the appropriate version of PINsafe Web Interface Integration on the PINsafe server see Integrations. Test that this integration is fully working.

35.2 CAG Standard and CAG VPX configuration and installation

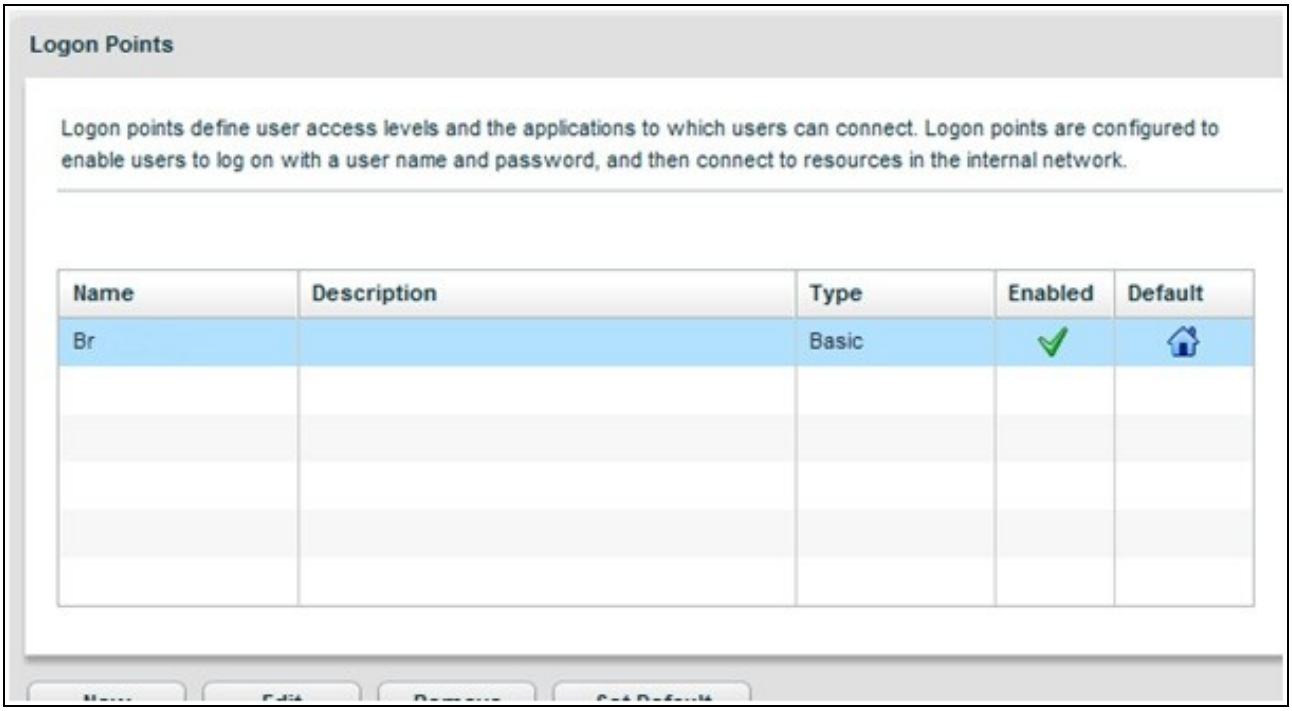
Configure the Access Gateway with networking information in the required deployment scenario. On the CAG enter under Name Service Providers the IP address and Fully Qualified Hostname of the Web Interface server under the section HOSTS File.



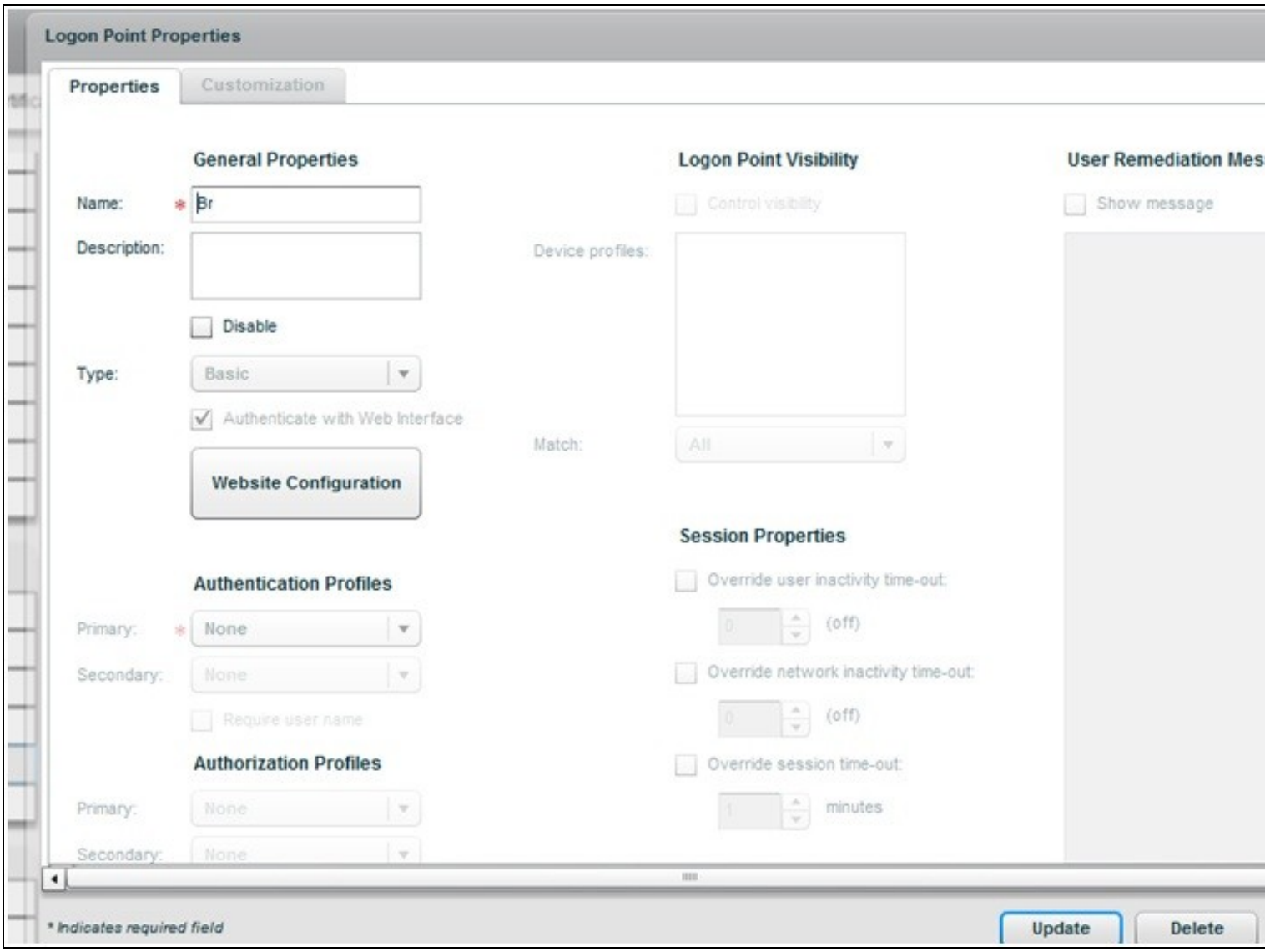
Under Deployment Mode set the Access Gateway Mode to Appliance Only.



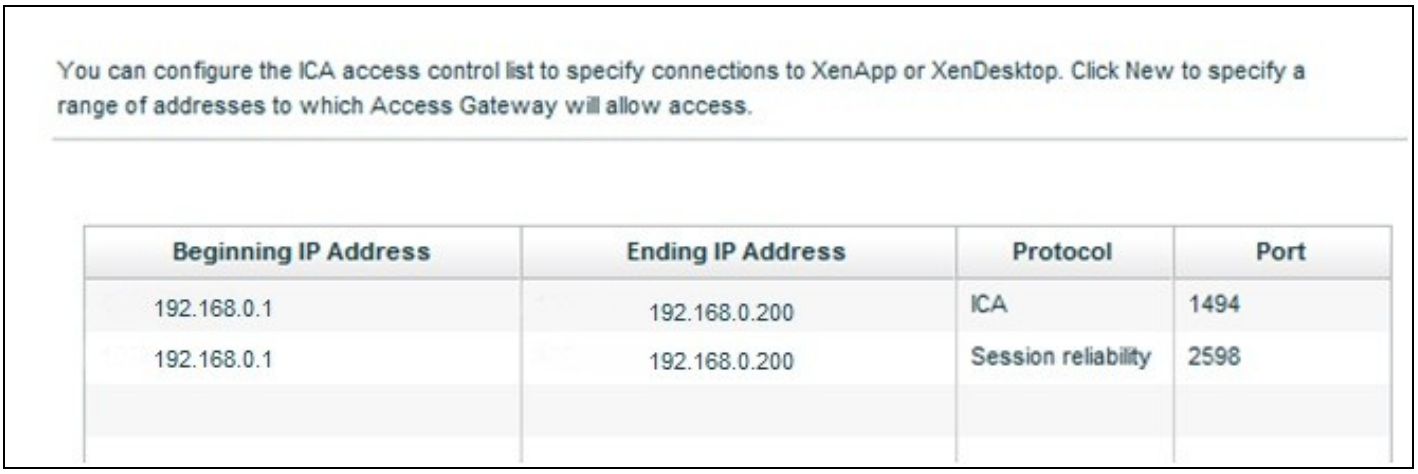
Set the Logon Point as home.



Configure the Logon Point Properties to authenticate with the Web Interface, using the hostname allows the DMZ IP address range to be hidden.



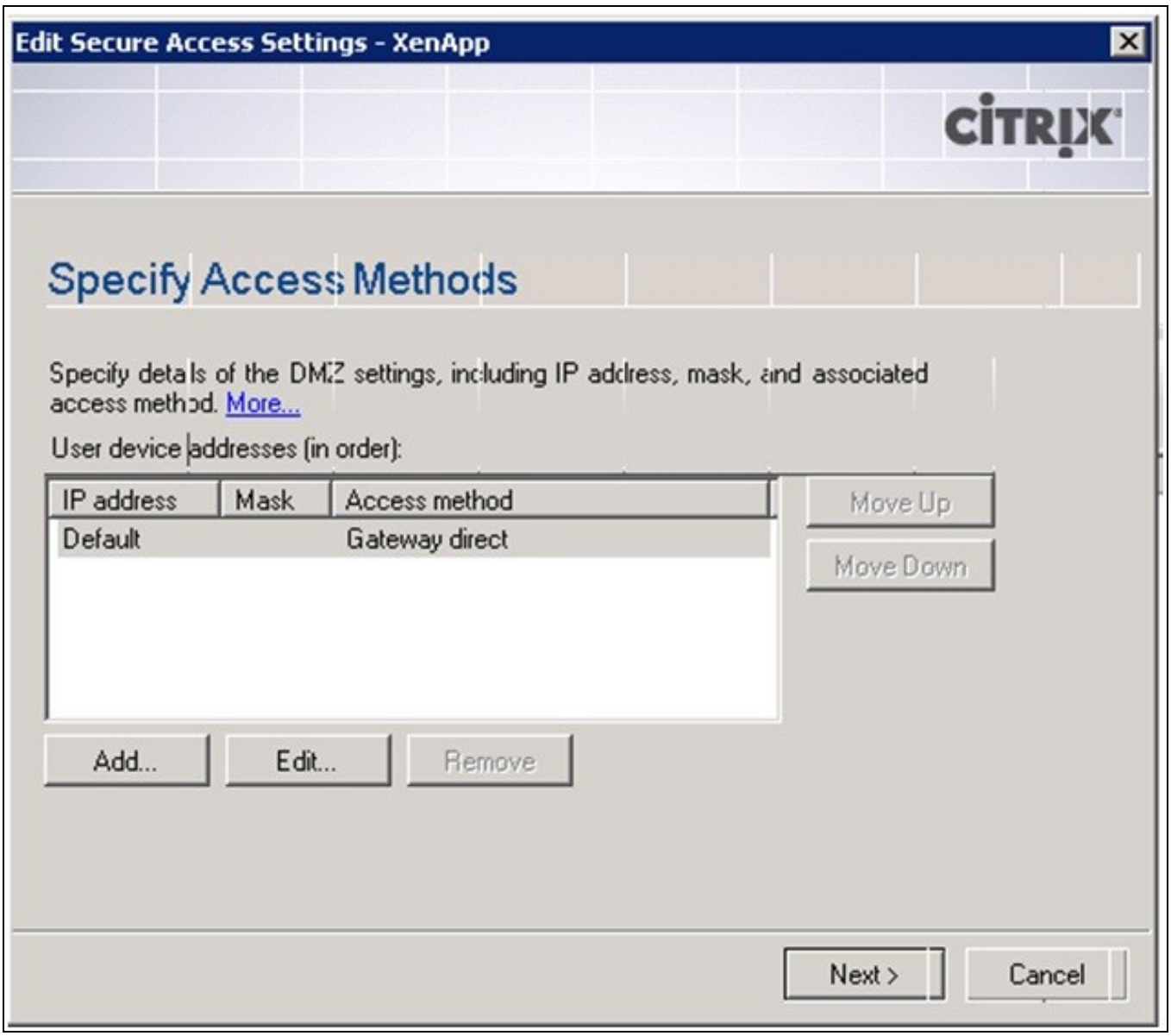
Enter the Web Interface server for the Web Address and Application Type should be WEBINTERFACE.



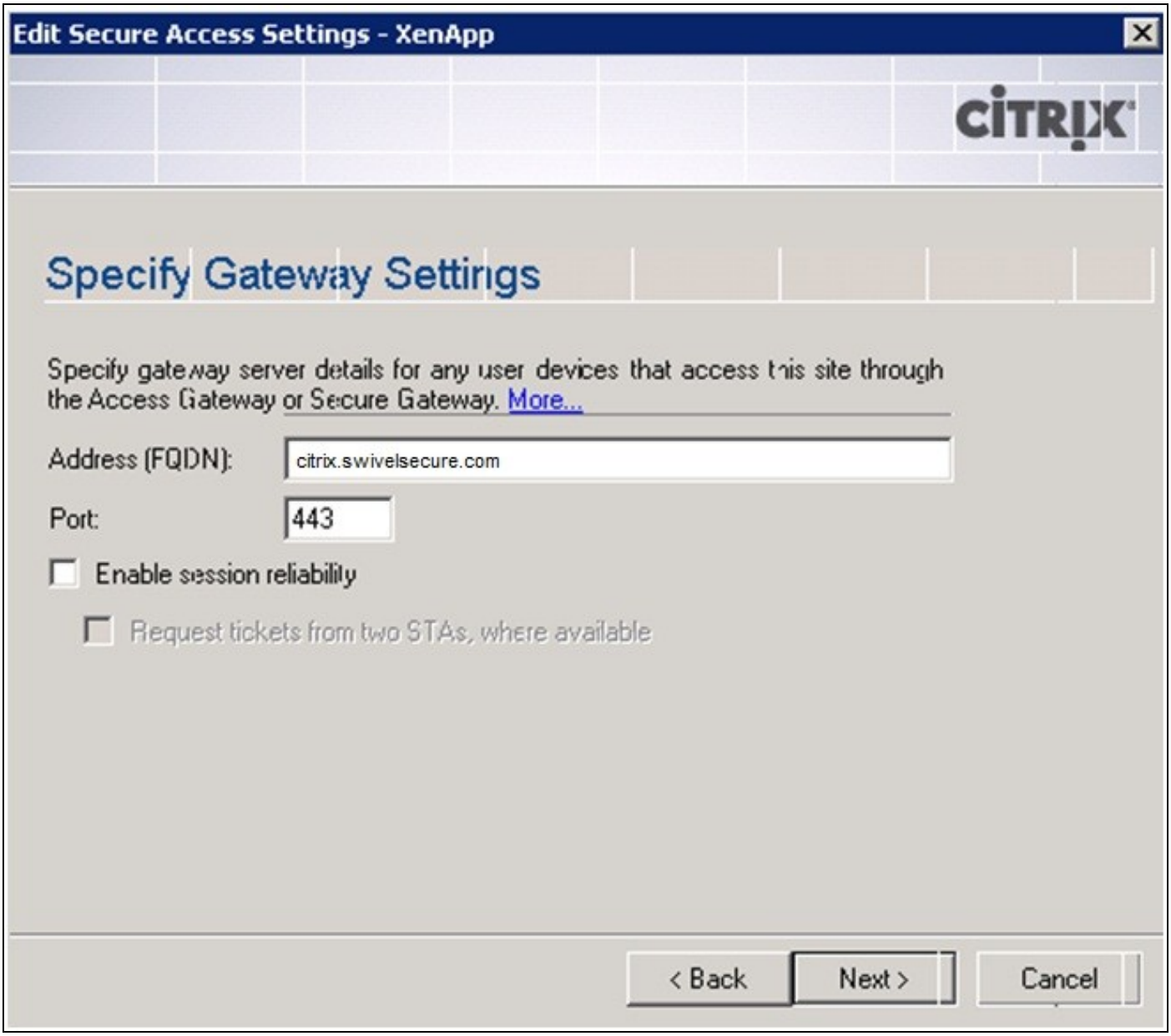
Configure the Web Interface as the STA (Secure Ticket Authority).

35.3 Citrix Web Interface configuration and installation

On the Citrix Web Interface edit the Secure Access Settings, Access Methods to be Gateway Direct.



The (FQDN) Fully Qualified Domain Name needs to be entered for the Gateway Settings



35.4 Additional Installation Options

36 Verifying the Installation

Browse to the login page and authenticate with PINsafe credentials.

37 Uninstalling the PINsafe Integration

38 Troubleshooting

39 Known Issues and Limitations

40 Additional Information