

Table of Contents

| | |
|---|-----------|
| 1 Citrix Access Gateway 5 VPX | 1 |
| 1.1 Introduction..... | 1 |
| 2 Citrix Access Gateway Access Controller 5.0 | 2 |
| 3 Citrix Access Gateway Advanced 4.x | 3 |
| 4 Introduction | 4 |
| 5 Prerequisites | 5 |
| 6 Installation | 6 |
| 7 Additional Installation Options | 7 |
| 7.1 Remove automatic TURING image automatically displaying..... | 7 |
| 7.2 Prevent browser caching TURING image..... | 7 |
| 7.3 Prevent the cursor from automatically entering the OTC field..... | 7 |
| 7.4 Change the TURING button text..... | 7 |
| 7.5 Verifying the Installation..... | 7 |
| 7.6 Uninstalling the PINsafe Integration..... | 7 |
| 7.7 Troubleshooting..... | 7 |
| 7.8 Known Issues and Limitations..... | 7 |
| 7.9 Additional Information..... | 7 |
| 8 Citrix Access Gateway Standard 4.x | 8 |
| 9 Introduction | 9 |
| 10 Prerequisites | 10 |
| 11 Baseline | 11 |
| 12 Architecture | 12 |
| 13 Installation | 13 |
| 14 Swivel Configuration | 14 |
| 14.1 Configuring the RADIUS server..... | 14 |
| 14.2 Setting up PINsafe Dual Channel Transports..... | 14 |
| 14.3 Citrix Access Gateway Standard Edition Integration..... | 14 |
| 15 Additional Information | 15 |
| 16 Citrix Access Gateway Standard 5.x | 16 |
| 17 Introduction | 17 |
| 18 Prerequisites | 18 |
| 19 Baseline | 19 |
| 20 Architecture | 20 |
| 21 Installation | 21 |
| 22 Swivel Configuration | 22 |
| 22.1 Configuring the RADIUS server..... | 22 |
| 22.2 Setting up PINsafe Dual Channel Transports..... | 22 |
| 23 Citrix Access Gateway Standard Edition Integration | 23 |
| 23.1 CAG RADIUS Properties..... | 23 |
| 23.2 CAG logon Point Properties..... | 23 |
| 24 Additional Installation Options | 25 |
| 25 Verifying the Installation | 26 |
| 26 Uninstalling the PINsafe Integration | 27 |
| 27 Troubleshooting | 28 |
| 28 Known Issues and Limitations | 29 |
| 29 Additional Information | 30 |
| 30 Citrix Access Gateway Web Interface Proxy | 31 |
| 31 Introduction | 32 |
| 32 Prerequisites | 33 |
| 33 Baseline | 34 |

Table of Contents

| | |
|---|-----------|
| 34 Architecture..... | 35 |
| 35 Installation..... | 36 |
| 35.1 PINsafe and Web Interface Integration Configuration..... | 36 |
| 35.2 CAG Standard and CAG VPX configuration and installation..... | 36 |
| 35.3 Citrix Web Interface configuration and installation..... | 39 |
| 35.4 Additional Installation Options..... | 40 |
| 36 Verifying the Installation..... | 41 |
| 37 Uninstalling the PINsafe Integration..... | 42 |
| 38 Troubleshooting..... | 43 |
| 39 Known Issues and Limitations..... | 44 |
| 40 Additional Information..... | 45 |

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](#)

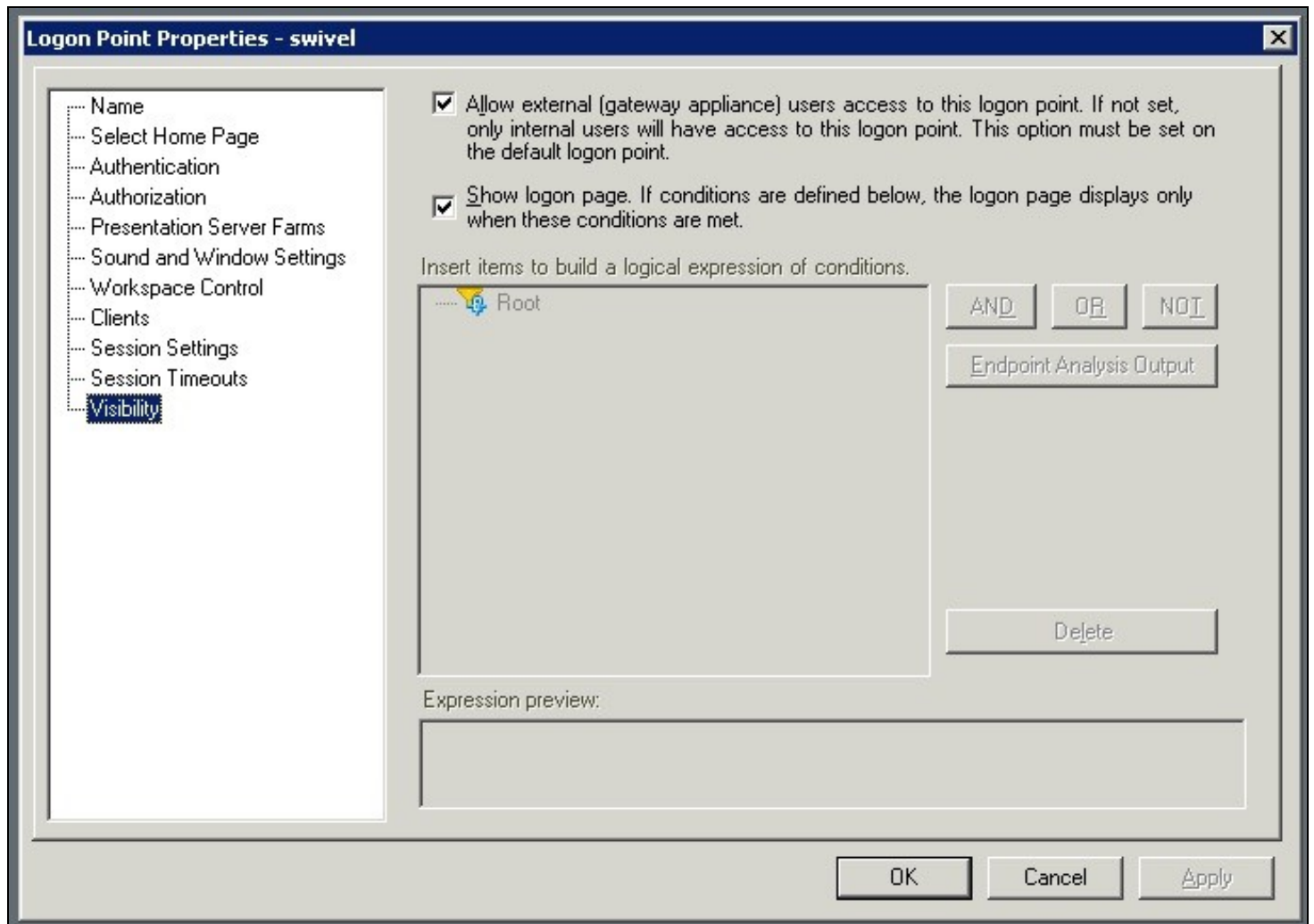
The CAG 4.5.8 integration guide is available here: [Citrix Access Gateway Advanced edition 4.5.8](#)

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.

RADIUS Properties

General Properties

Profile name: * Swivel

Description: Swivel

Single sign-on domain: IGroup

RADIUS Servers

Network time-out: 5 seconds

Servers list: *

| Server | Port | Accounting | Priority |
|---------|------|------------|----------|
| 1.1.1.1 | 1812 | 1813 | 1 |
| | | | |
| | | | |

New Remove Move: ↑ ↓

Group Authorization

Attribute value prefix: CTXSUserGroups=

Separator: ;

Vendor attribute: 0

Vendor code:

* Indicates required field

Update Delete Cancel

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: *

Description:

Disable

Type:

Authenticate with Web Interface

Web Interface: *

Authentication Profiles

Primary: *

Secondary:

Require user name

Single sign-on to Web Interface

Authorization Profiles

Primary:

Secondary:

Logon Point Visibility

Control visibility

Device profiles:

Match:

Session Properties

Override user inactivity time-out: (off)

Override network inactivity time-out: (off)

Override session time-out: minutes

User Remediation Message

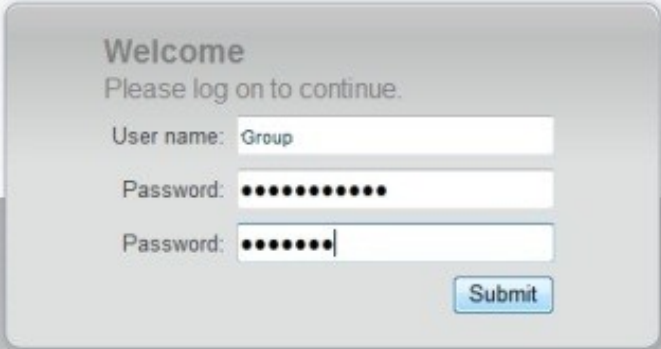
Show message

* Indicates required field

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.



A screenshot of a Citrix login dialog box. The dialog box is titled "Welcome" and contains the text "Please log on to continue." Below this text are three input fields: "User name:" with the text "Group" entered, "Password:" with ten black dots, and another "Password:" field with seven black dots. A "Submit" button is located to the right of the second password field. The Citrix logo is visible at the bottom center of the background.

citrix

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.

Name Service Providers

If you use domain name servers (DNS) or Windows Internet Name Service (WINS) servers, specify the IP addresses for these servers.

| Domain Name Servers | | WINS Server |
|---------------------|--------------------------------------|----------------------|
| First DNS Server: | <input type="text" value="8.8.8.8"/> | <input type="text"/> |
| Second DNS Server: | <input type="text" value="8.8.4.4"/> | |
| Third DNS Server: | <input type="text"/> | |

| HOSTS File | | DNS Suffixes | | | | | | | | | | | | | | | | | | |
|--|-----------------------------|--|---------------|--------|--|--|--|--|--|--------|----------|--|--|--|--|--|--|------------------------------------|---------------------------------------|---|
| <i>Click New to add the IP address and fully qualified domain name to the HOSTS file.</i> | | <i>Do not precede a suffix with a period. Specify the DNS server as site.com, not .site.com.</i> | | | | | | | | | | | | | | | | | | |
| <table border="1"><thead><tr><th>IP Address</th><th>Fully qualified domain name</th></tr></thead><tbody><tr><td>192.168.1.102</td><td>TSWDMZ</td></tr><tr><td> </td><td> </td></tr><tr><td> </td><td> </td></tr></tbody></table> | IP Address | Fully qualified domain name | 192.168.1.102 | TSWDMZ | | | | | <table border="1"><thead><tr><th>Suffix</th><th>Priority</th></tr></thead><tbody><tr><td> </td><td> </td></tr><tr><td> </td><td> </td></tr><tr><td> </td><td> </td></tr></tbody></table> | Suffix | Priority | | | | | | | <input type="button" value="New"/> | <input type="button" value="Remove"/> | Move: <input type="button" value="↑"/> <input type="button" value="↓"/> |
| IP Address | Fully qualified domain name | | | | | | | | | | | | | | | | | | | |
| 192.168.1.102 | TSWDMZ | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| Suffix | Priority | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | |

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

Deployment Mode

Configure the settings to use the Delivery Services Console for Access Controller to configure the Access Gateway appliance.

Access Gateway Settings

Identifier: *

Access Gateway mode: Appliance only Access Controller

Select your preferred mode for configuring settings to manage Access Gateway.

Access Controller Settings

Shared key: *

Server address: *

Secure connection


Port: *

* Indicates required field

Set the Logon Point as home.

Logon Points

Logon points define user access levels and the applications to which users can connect. Logon points are configured to enable users to log on with a user name and password, and then connect to resources in the internal network.

| Name | Description | Type | Enabled | Default |
|------|-------------|-------|---------|---|
| Br | | Basic | ✓ |  |
| | | | | |
| | | | | |
| | | | | |

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

Logon Point Properties

Properties | Customization

General Properties

Name: *

Description:

Disable

Type:

Authenticate with Web Interface

Website Configuration

Logon Point Visibility

Control visibility

Device profiles:

Match:

User Remediation Mes

Show message

Authentication Profiles

Primary: *

Secondary:

Require user name

Authorization Profiles

Primary:

Secondary:

Session Properties

Override user inactivity time-out: (off)

Override network inactivity time-out: (off)

Override session time-out: minutes

* Indicates required field

Update **Delete**

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

You can configure the ICA access control list to specify connections to XenApp or XenDesktop. Click New to specify a range of addresses to which Access Gateway will allow access.

| Beginning IP Address | Ending IP Address | Protocol | Port |
|----------------------|-------------------|---------------------|------|
| 192.168.0.1 | 192.168.0.200 | ICA | 1494 |
| 192.168.0.1 | 192.168.0.200 | Session reliability | 2598 |
| | | | |
| | | | |

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

Secure Ticket Authority

The Secure Ticket Authority (STA) issues tickets in response to connection requests for published applications on XenApp configured in the Web Interface. Click **New** to configure STA servers on Access Gateway.

| Server | Port | Path | Identifier | Connection Type |
|-------------|------|---------------------|------------|-----------------|
| 192.168.0.1 | 8080 | /Scripts/CtxSTA.dll | STA150 | unsecure |
| | | | | |
| | | | | |

35.3 Citrix Web Interface configuration and installation

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

Edit Secure Access Settings - XenApp

CITRIX

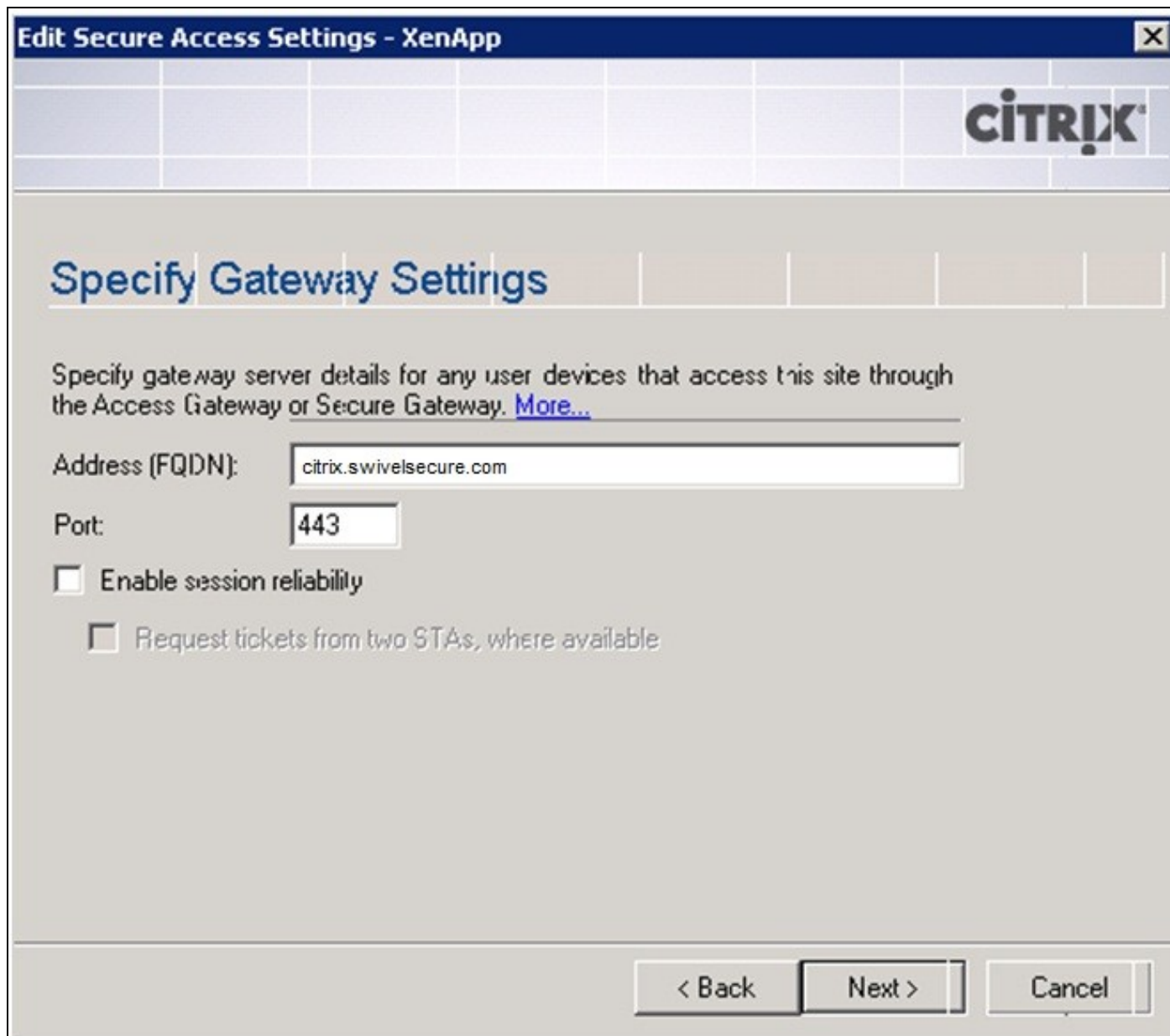
Specify Access Methods

Specify details of the DMZ settings, including IP address, mask, and associated access method. [More...](#)

User device addresses (in order):

| IP address | Mask | Access method |
|------------|------|----------------|
| Default | | Gateway direct |
| | | |

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



The screenshot shows a window titled "Edit Secure Access Settings - XenApp" with the Citrix logo in the top right corner. The main heading is "Specify Gateway Settings". Below this, there is a descriptive paragraph: "Specify gateway server details for any user devices that access this site through the Access Gateway or Secure Gateway. [More...](#)".

The form contains the following fields and options:

- Address (FQDN):** A text input field containing "citrix.swivelsecure.com".
- Port:** A text input field containing "443".
- Enable session reliability**
- Request tickets from two STAs, where available*

At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

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