Citrix Access Gateway Web Interface Proxy

Contents

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.

Prerequisites

Citrix Access Gateway 5.x

Citrix Web Interface 5.x

PINsafe 3.x

Baseline

Citrix Access Gateway 5.0

Citrix Web Interface 5.4

PINsafe 3.8

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.

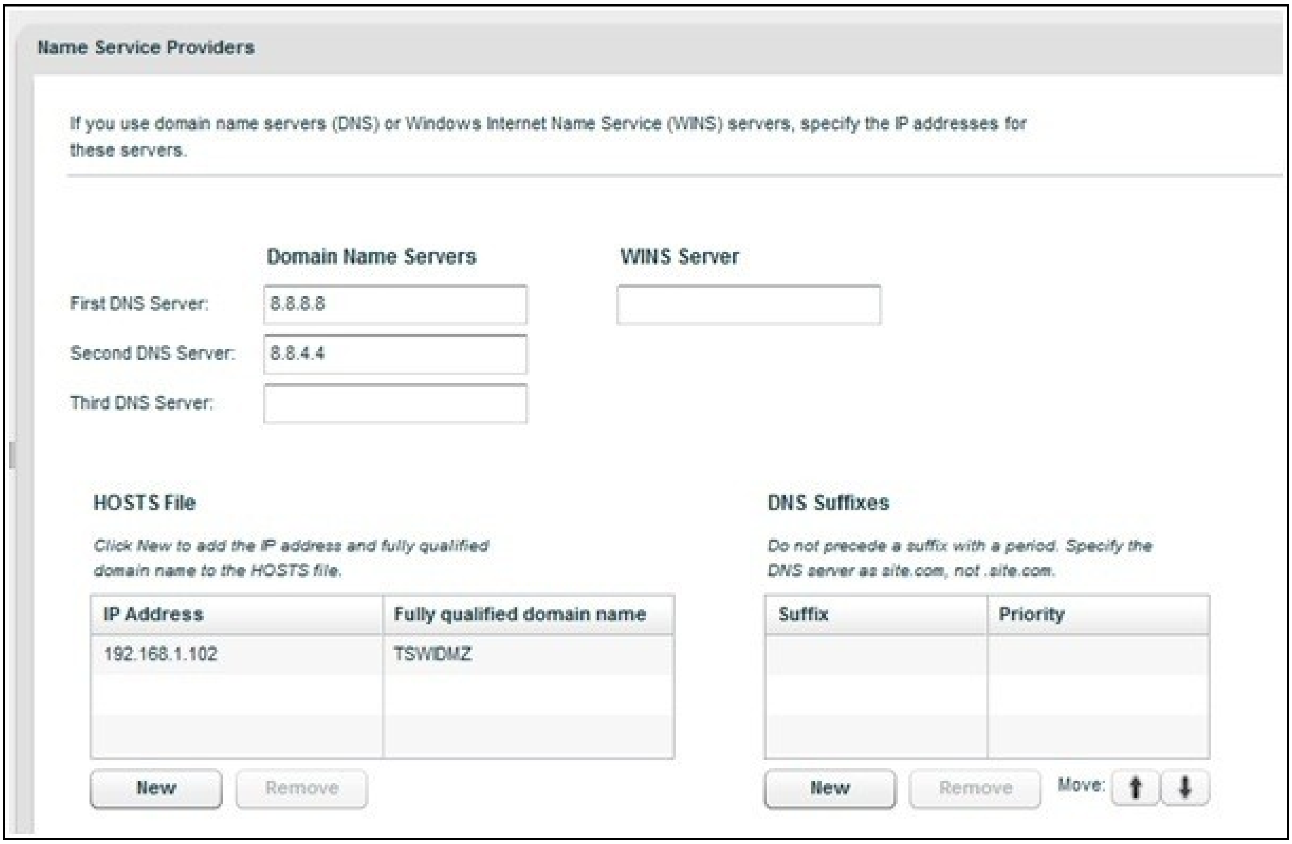
Installation

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.

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:	8.8.8.8	
Second DNS Server:	8.8.4.4	
Third DNS Server:		

HOSTS File

Click New to add the IP address and fully qualified domain name to the HOSTS file.

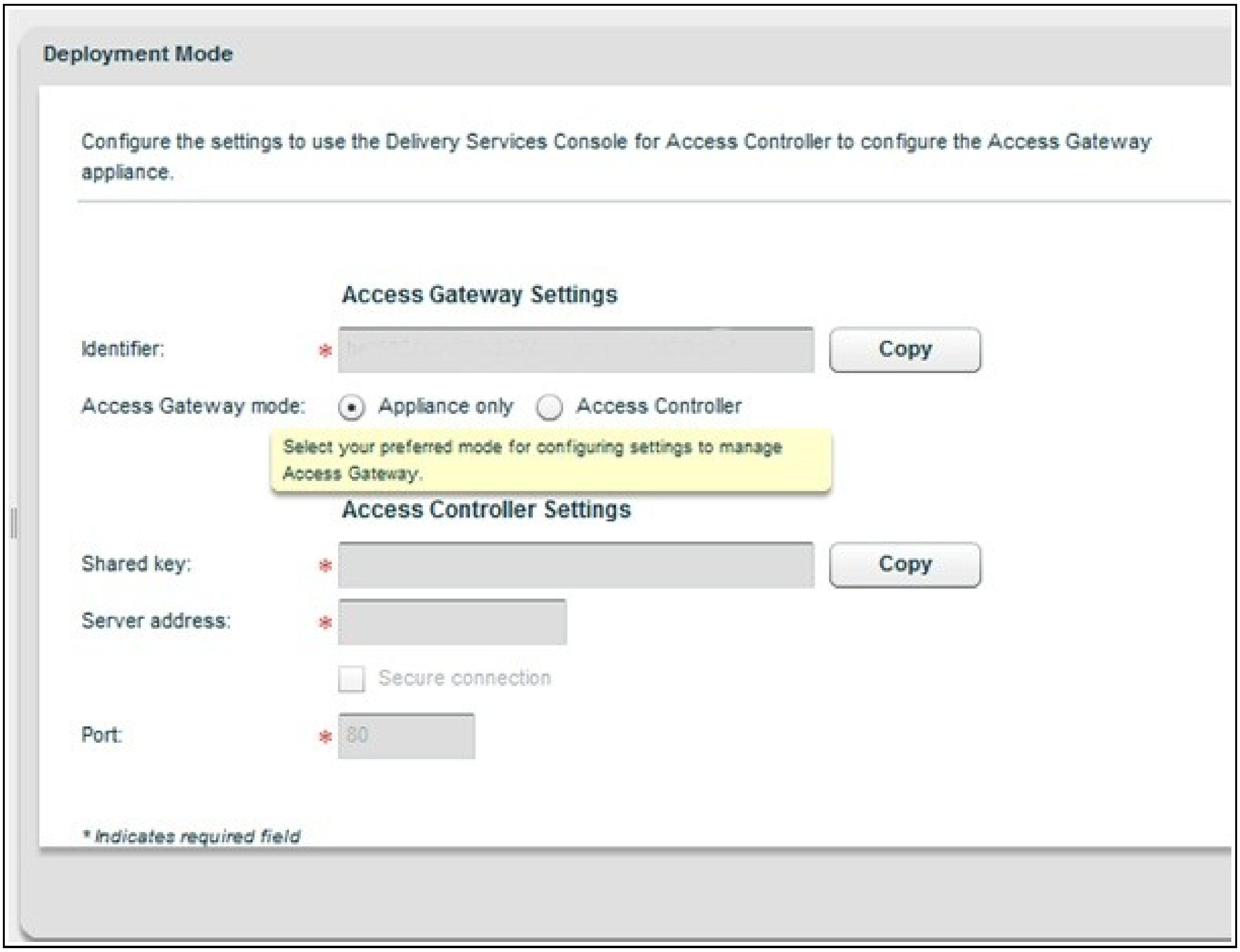
IP Address	Fully qualified domain name
192.168.1.102	TSWIDMZ

DNS Suffixes

Do not precede a suffix with a period. Specify the DNS server as site.com, not .site.com.

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: *

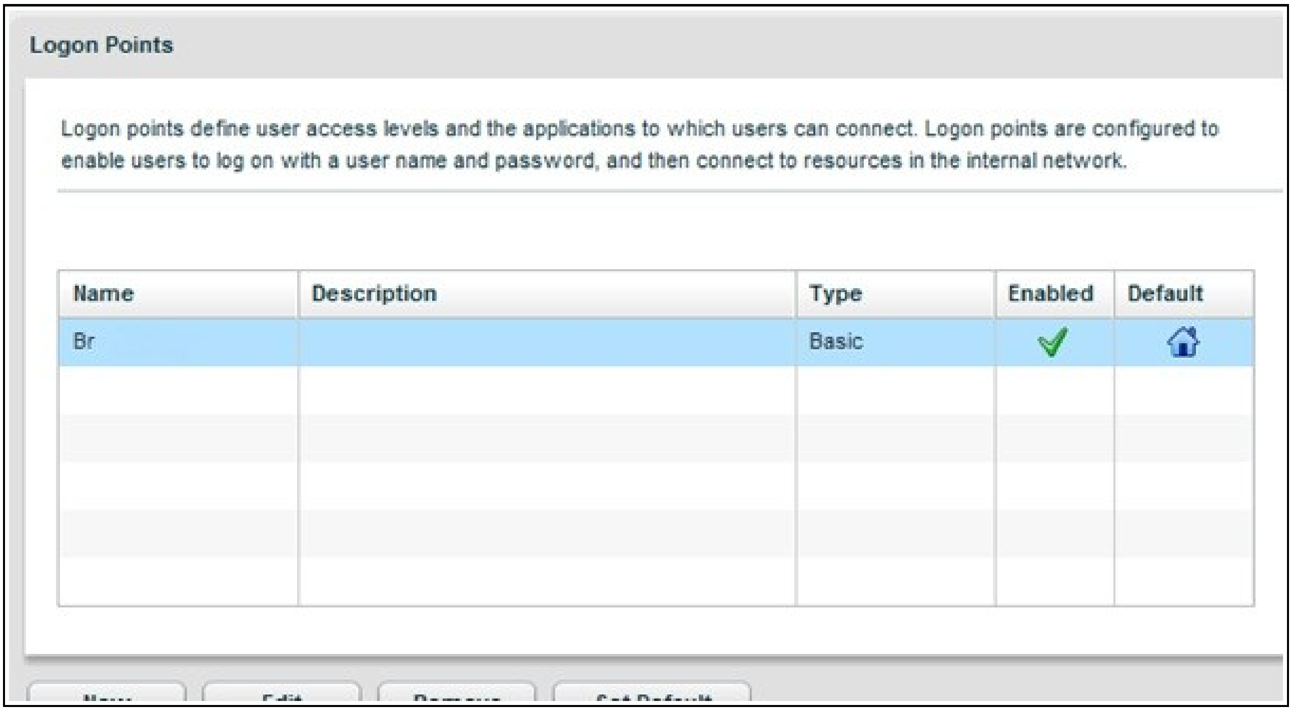
Server address: *

□ Secure connection

Port: * 80

** Indicates required field*

Set the Logon Point as home.

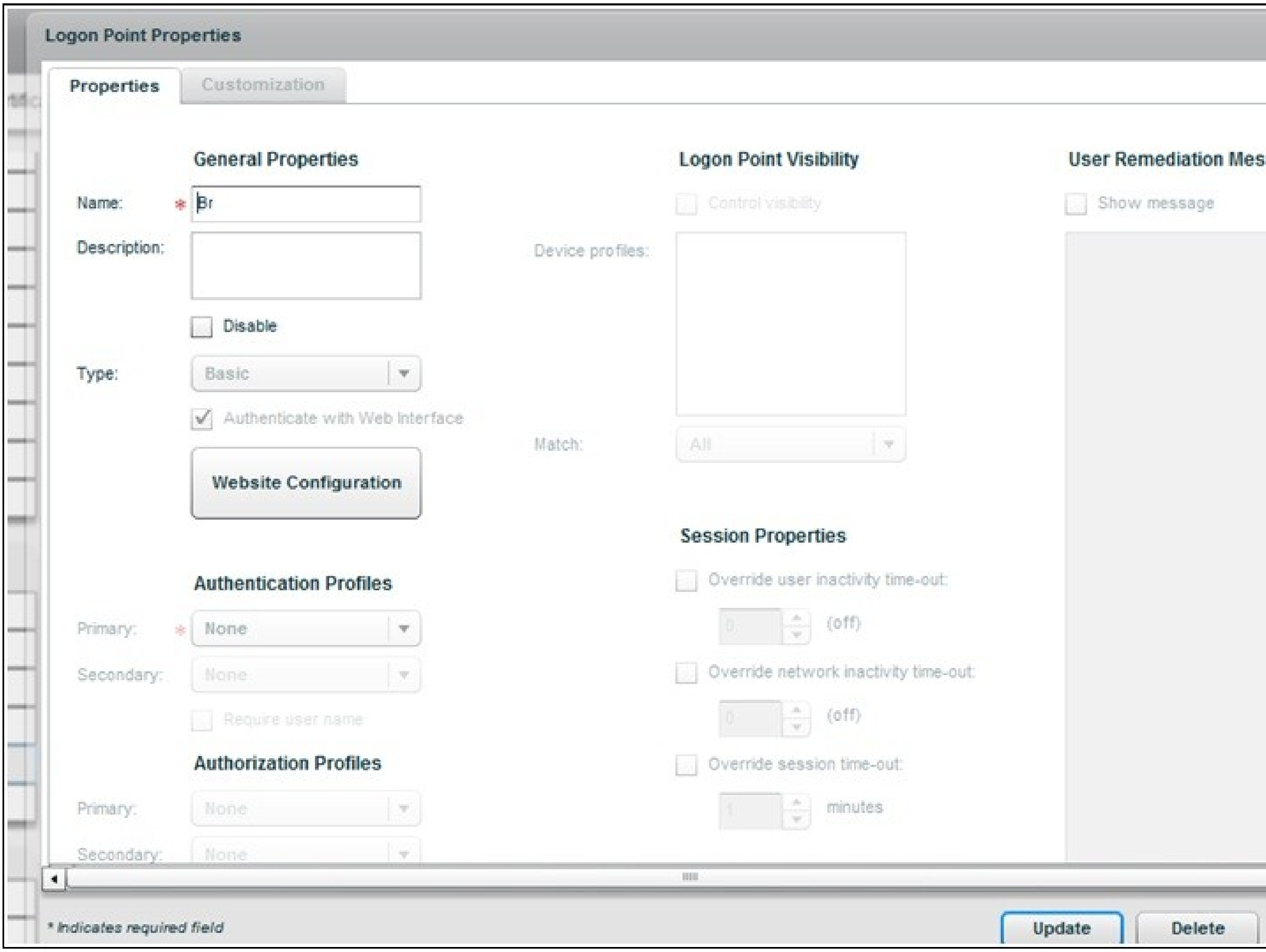


Logon Points

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: * Br

Description:

☐ Disable

Type: Basic

☑ Authenticate with Web Interface

Authentication Profiles

Primary: * None

Secondary: None

☐ Require user name

Authorization Profiles

Primary: None

Secondary: None

Logon Point Visibility

☐ Control visibility

Device profiles:

Match: All

Session Properties

☐ Override user inactivity time-out:

0 (off)

☐ Override network inactivity time-out:

0 (off)

☐ Override session time-out:

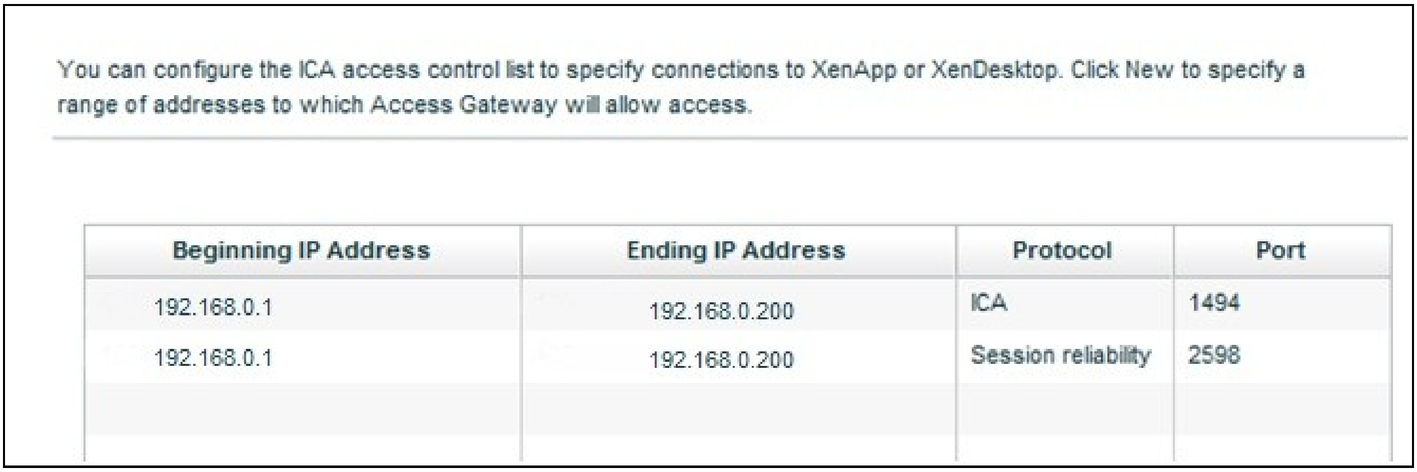
1 minutes

User Remediation Mes

☐ Show message

* Indicates required field

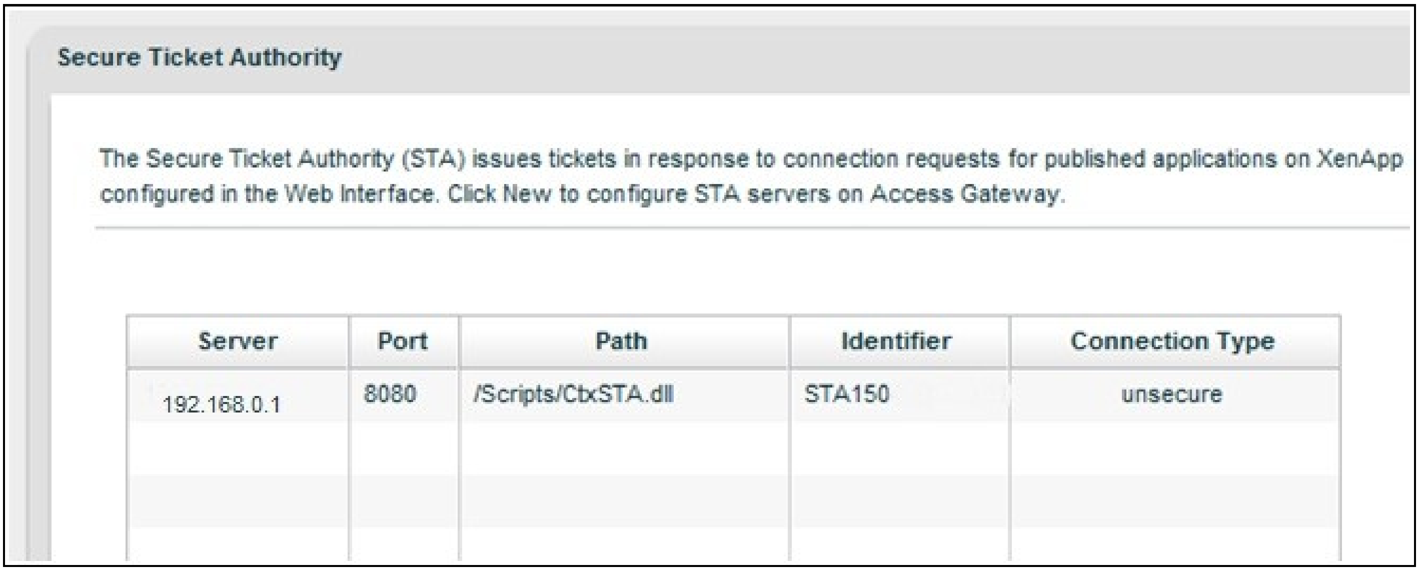
Enter the Web Interface server for the Web Address and Application Type should be WEBINTERFACE.



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).



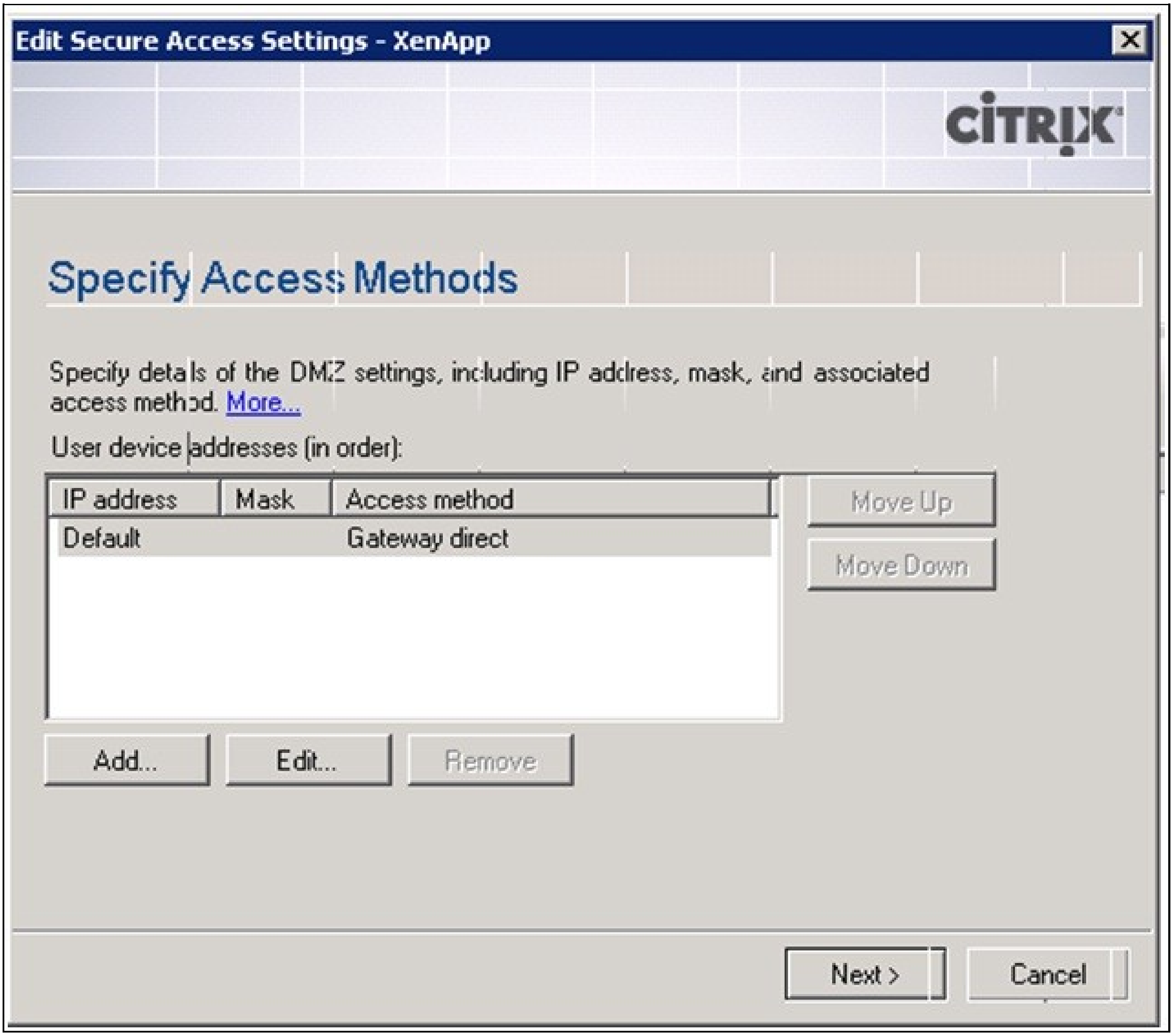
Secure Ticket Authority

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

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

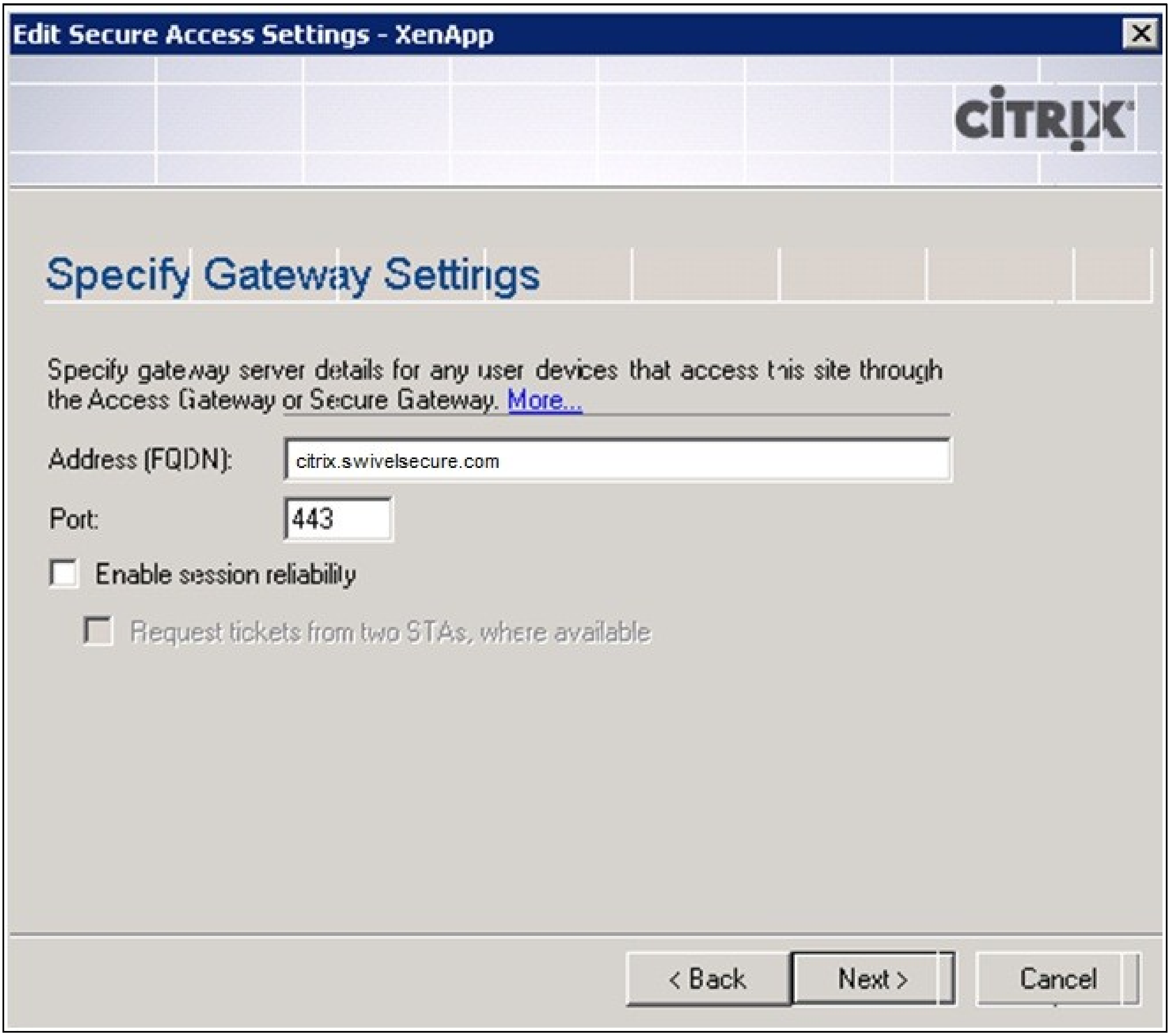
Specify Access Methods

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



Specify gateway server details for any user devices that access this site through the Access Gateway or Secure Gateway. More...

Address (FQDN): citrix.swivelsecure.com

Port: 443

□ Enable session reliability

□ Request tickets from two STAs, where available

Additional Installation Options

Verifying the Installation

Browse to the login page and authenticate with PINsafe credentials.

Uninstalling the PINsafe Integration

Troubleshooting

Known Issues and Limitations

Additional Information