SafeNet Authentication Service

Integration Guide

Citrix Access Gateway

Document Information

Document Part Number	007-012638-001, Rev A
Release Date	July 2014

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Citrix Access Gateway.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

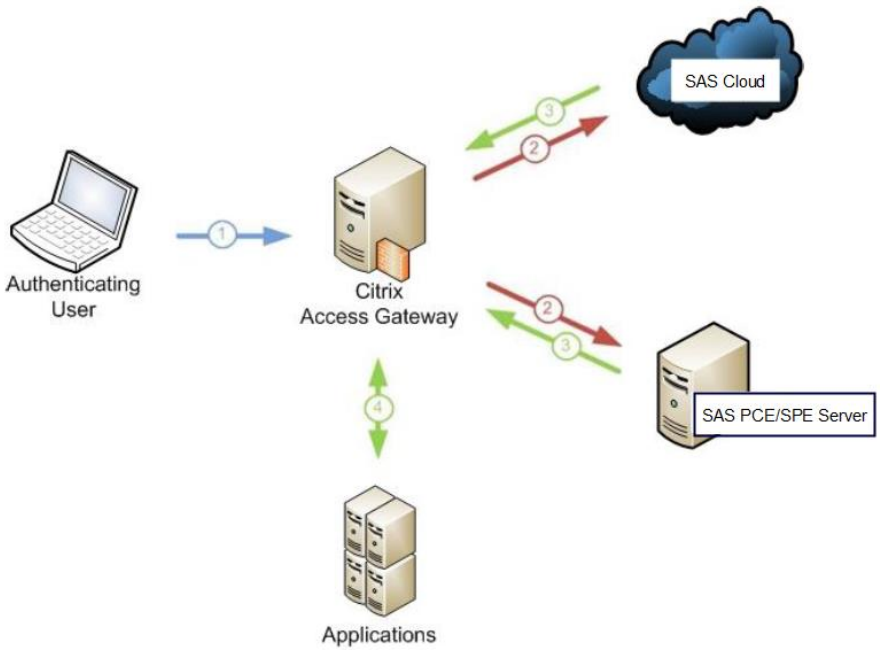
Applicability

This Integration Guide is applicable to the following authentication servers:

- SafeNet Authentication Service Cloud
- SafeNet Authentication Service PCE/SPE

Solution Overview

1. User browses to the Citrix Access Gateway (CAG), which presents them with a logon screen. User enters username and one-time password (OTP).
2. The Citrix Access Gateway sends the authentication request via RADIUS to either:
    - SAS Cloud
    - SAS PCE/SPE
3. The authentication service/server verifies the username and OTP and sends an Access-Accept to CAG if authentication is successful.
4. CAG grants user access on receipt of the Access-Access message.



The authentication server and Citrix Access Gateway must be configured to use RADIUS authentication.

Resource	Authentication Server/Service	Citrix Access Gateway
Address	IP Address of Citrix Access Server	IP Address of Authentication Server/Service
Port	1812	
Shared Secret	Shared Secret Value	

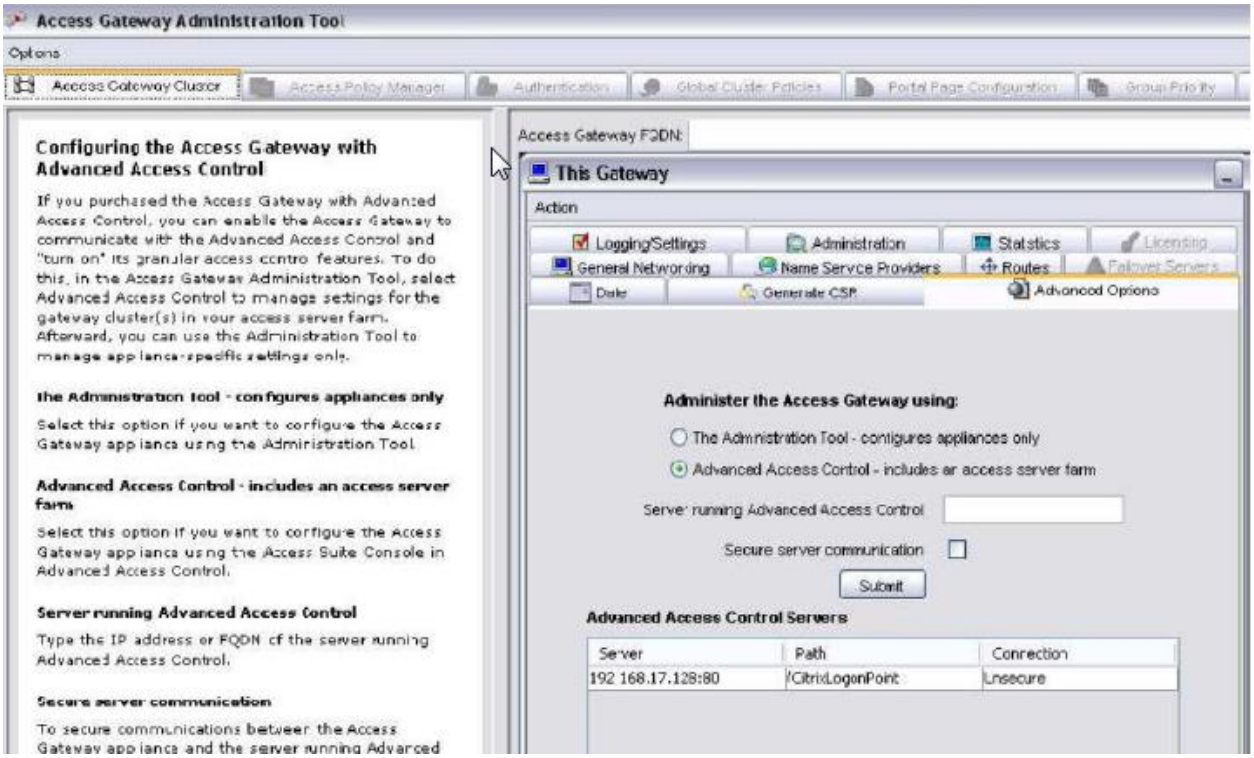
It is recommended to test authentication using a static password prior to testing using one-time passwords.

Configuring CAG without AAC

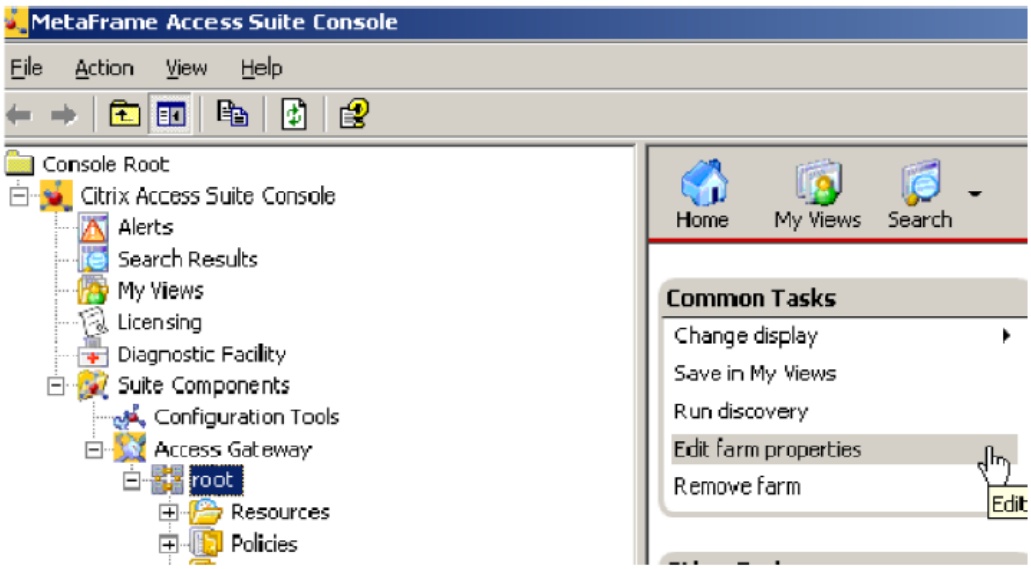
1. Open the Citrix Access Gateway Administration Tool.
2. Click on the **Authentication** tab.
3. Click on the second **Authentication** tab. Select **Default** or create a new realm.
4. Configure Radius Parameters.

Enabling AAC for CAG

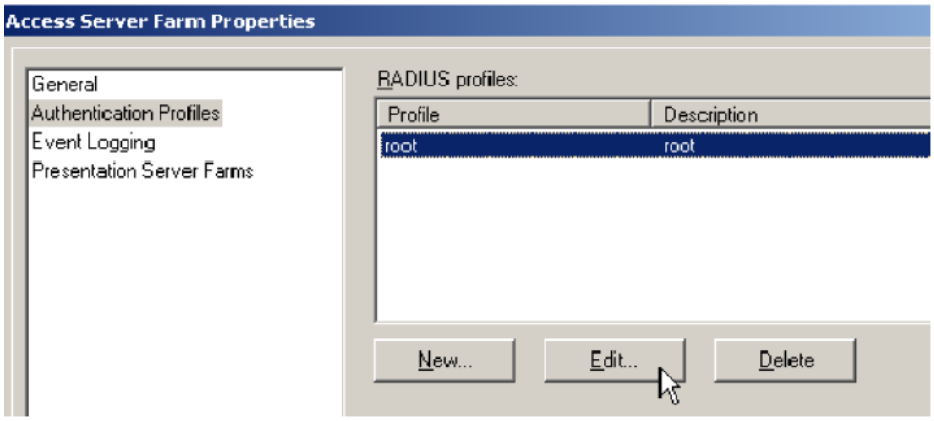
1. Open the Citrix Access Gateway Administration Tool.
2. Click **Access Gateway Cluster**.
3. Click **Advanced Options > Advanced Access Control**. Enter the IP Address or Hostname of the server running Advanced Access Control.



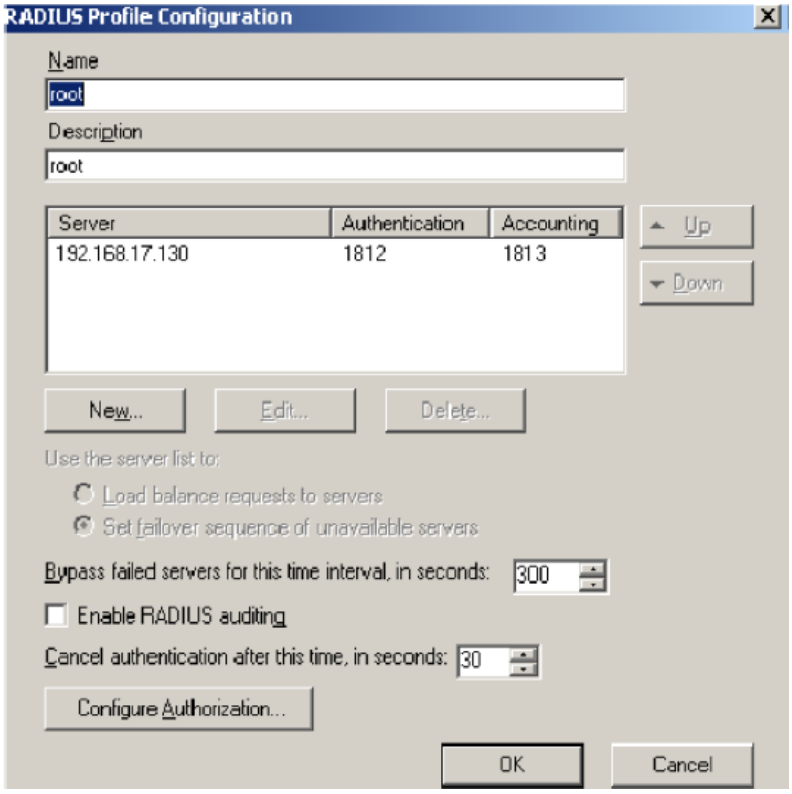
4. Open the Citrix Access Suite Console.
5. Select your farm (in the following example, the farm name is “root”) and then select **Edit Farm Properties**.



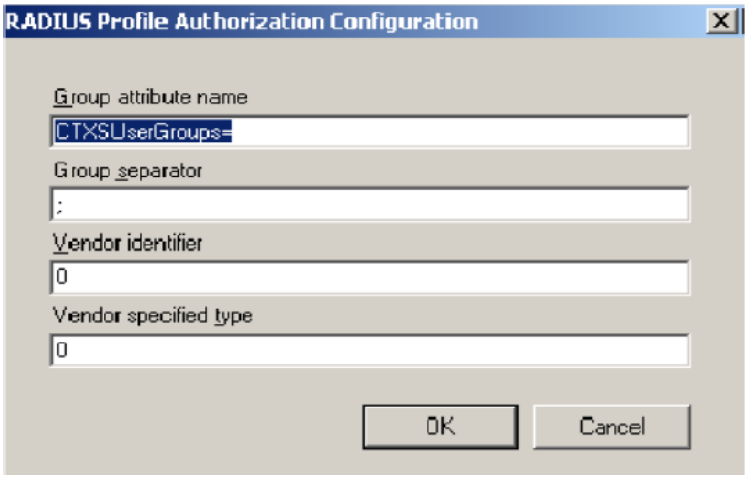
6. Select **New** and then click **Edit**.



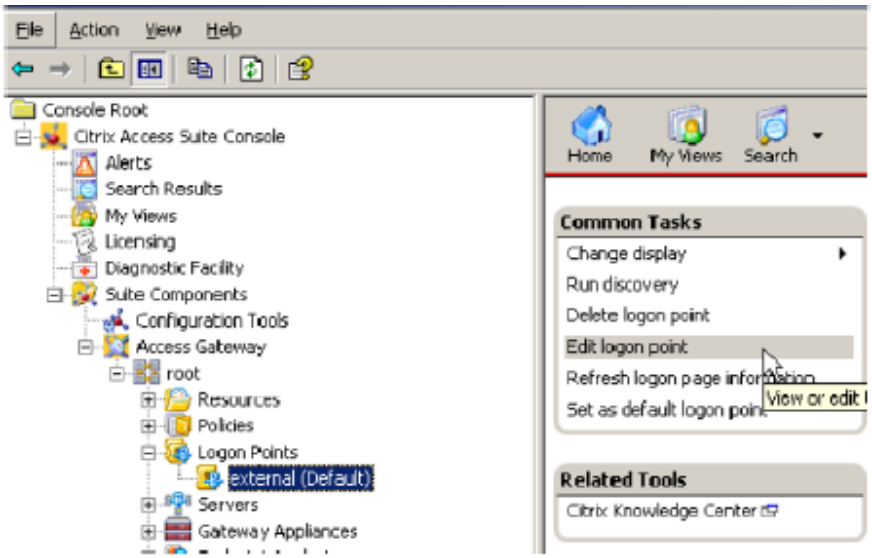
7. Enter your RADIUS profile configuration.

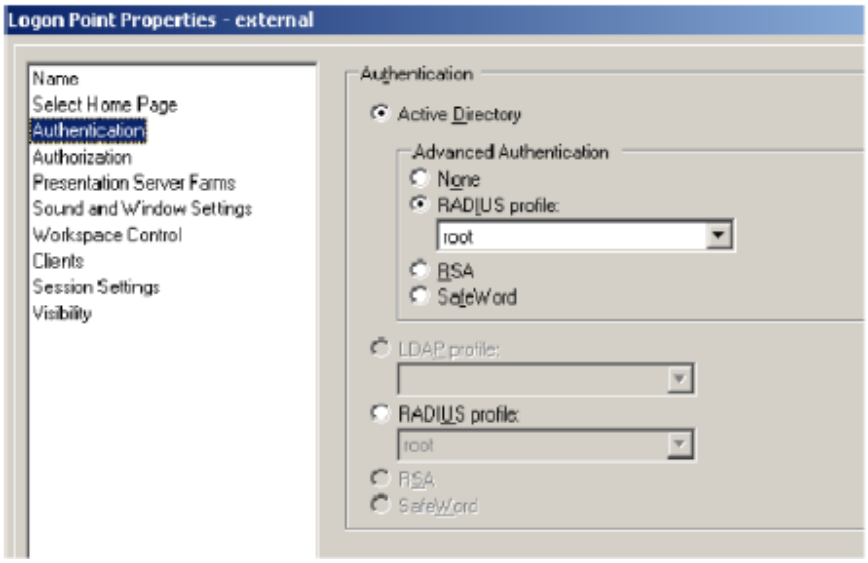


8. Select **Configure Authorization** and select the following information:

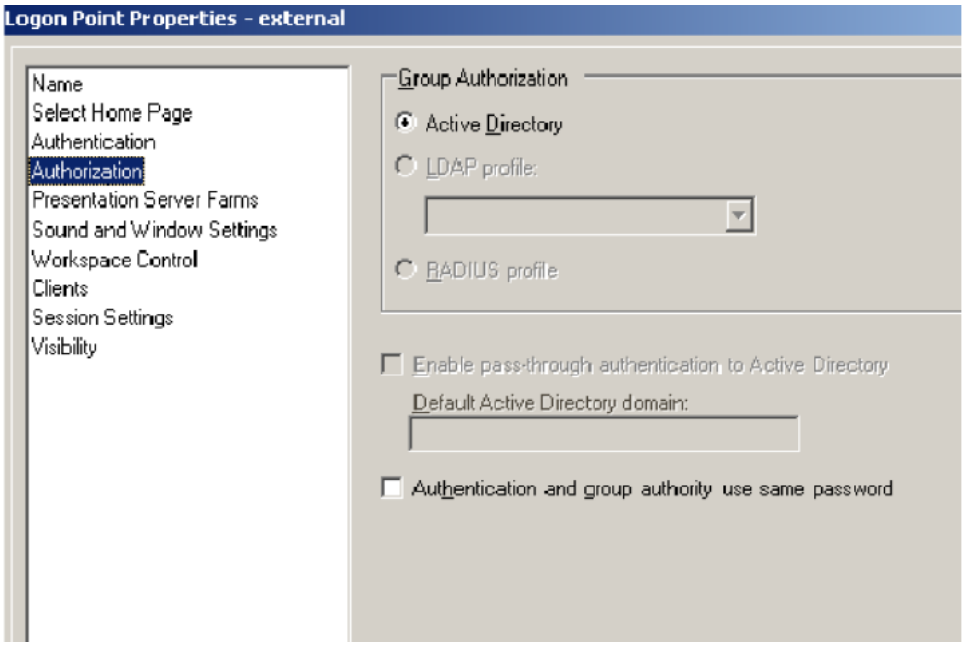


9. Return to the main window of the Citrix Access Suite, locate your Logon Point, and define a “default” Logon Point. Edit the Logon Point:





10. Add **Authorization** as required.



Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when phone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	