SafeNet Authentication Service

Integration Guide

Using RADIUS Protocol for Ericom PowerTerm WebConnect

security to be free

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Document Part Number: 007-013265-001, Rev. A

Release Date: August 2015

Contents

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Ericom PowerTerm WebConnect.

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.

Description

SafeNet Authentication Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

Ericom‘s PowerTerm WebConnect is a connection broker that manages access for various types of hosting platforms, such as Remote Desktop Session Hosts (Terminal Services), Virtual Desktop Infrastructure (VDI) and Legacy Systems. PowerTerm WebConnect enables IT administrators to get the most out of their Terminal Servers and VDI environments with minimal effort, while reducing complexity in managing access to applications, desktops, and documents.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Ericom PowerTerm WebConnect using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure Ericom PowerTerm WebConnect to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Ericom PowerTerm WebConnect environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Ericom PowerTerm WebConnect can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet’s cloud-based authentication service.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by Service Providers to deploy instances of SafeNet Authentication Service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version that is used to deploy the solution on-premises in the organization

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service (SAS)**—Version 3.3
- **Ericom PowerTerm WebConnect**—Version 6.0.0.0
- **Ericom Secure Gateway**—Version 7.1.0.0
- **Ericom AccessPortal for WebConnect**—Version 6.0.0.0

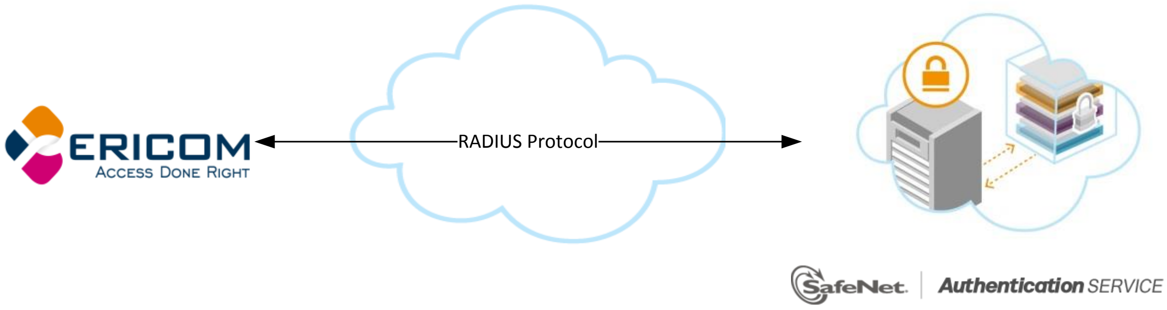
Audience

This document is targeted to system administrators who are familiar with Ericom PowerTerm WebConnect, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

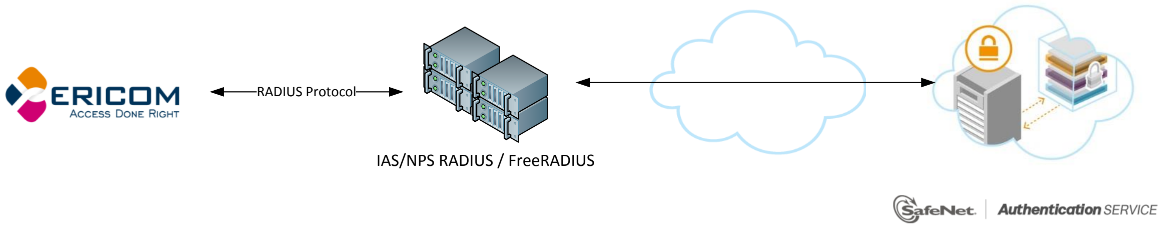
RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service**—A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.



- **Local RADIUS hosted on-premises**—A RADIUS agent that is implemented in the existing customer's RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.



This document demonstrates the solution using the SAS cloud hosted RADIUS service.

For more information on how to install and configure SAS Agent for IAS/NPS, refer to: http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

For more details on how to install and configure FreeRADIUS, refer to the *SafeNet Authentication Service FreeRADIUS Agent Configuration Guide*.

RADIUS-based Authentication using SAS-SPE and SAS-PCE

For both on-premises versions, SAS can be integrated with the following solutions that serve as local RADIUS servers:

- **Microsoft Network Policy Server (MS-NPS) or the legacy Microsoft Internet Authentication Service (MS-IAS)**—SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.

  For more information on how to install and configure the SAS Agent for Microsoft IAS and NPS, refer to the following document:

  http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

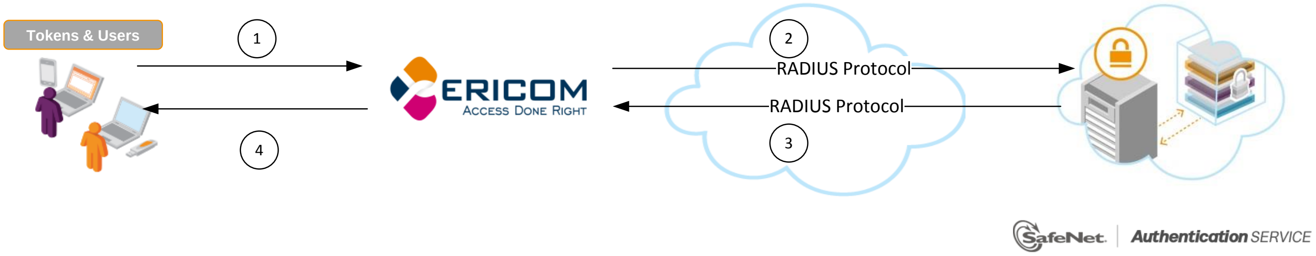
- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

RADIUS Authentication Flow using SAS

SafeNet Authentication Service communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the data flow of a multi-factor authentication transaction for Ericom PowerTerm WebConnect.



1. A user attempts to log on to Ericom PowerTerm WebConnect using his organizational credentials and an OTP authenticator.
2. Ericom PowerTerm WebConnect sends a RADIUS request with the user's credentials to SafeNet Authentication Service for validation.
3. The SAS authentication reply is sent back to Ericom PowerTerm WebConnect.
4. The user is granted or denied access to Ericom PowerTerm WebConnect based on the OTP value calculation results from SAS and his organization's Active Directory.

RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Ericom PowerTerm WebConnect, ensure the following:

- End users can authenticate from the Ericom PowerTerm WebConnect environment with a static password before configuring the Ericom PowerTerm WebConnect to use RADIUS authentication.
- Ports 1812/1813 are open to and from Ericom PowerTerm WebConnect.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Ericom PowerTerm WebConnect using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding Ericom PowerTerm WebConnect as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS Server's IP Address, page 11

Creating Users Stores in SAS

Before SAS can authenticate any user in your organization, you must create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time, using the **Create User** shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory / LDAP server using the SAS Synchronization Agent

For additional details on importing users to SafeNet Authentication Service, refer to "Creating Users" in the *SafeNet Authentication Service Subscriber Account Operator Guide*:

http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning an Authenticator in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Ericom PowerTerm WebConnect.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet GOLD
- SMS Token
- MP-1 Software Token
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

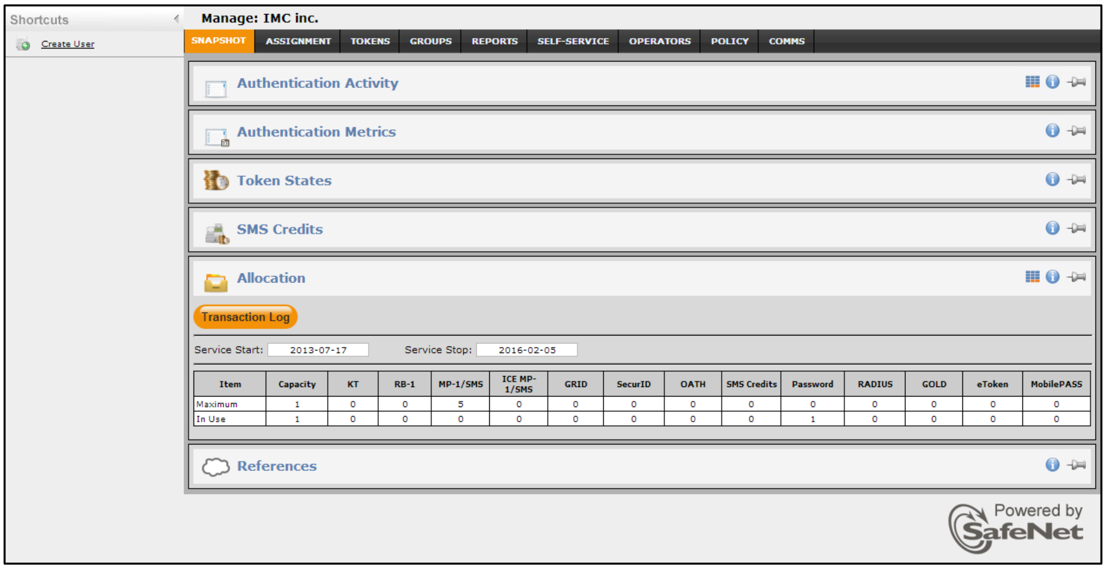
Refer to “Provisioning Rules” in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.

http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

Adding Ericom PowerTerm WebConnect as an Authentication Node in SAS

Add a RADIUS entry in the SAS **Auth Nodes** module to prepare it to receive RADIUS authentication requests from Ericom PowerTerm WebConnect. You will need the IP address of Ericom PowerTerm WebConnect and the shared secret to be used by both SAS and Ericom PowerTerm WebConnect.

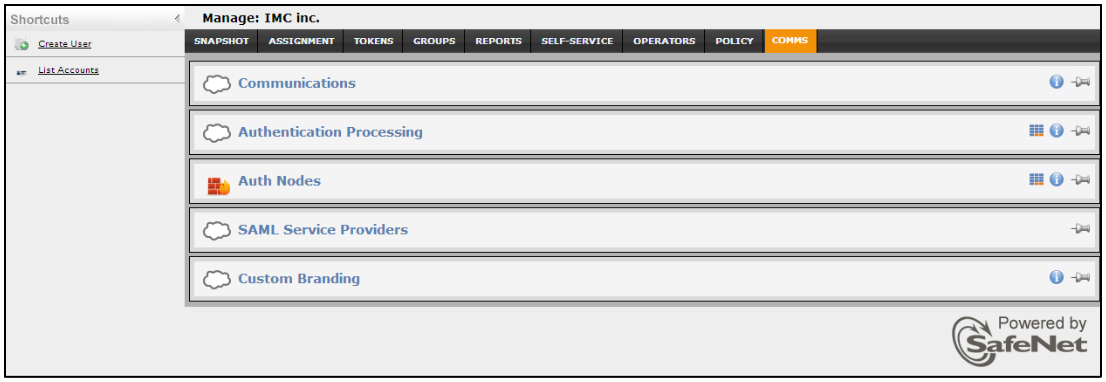
1. Log in to the SAS console with an Operator account.



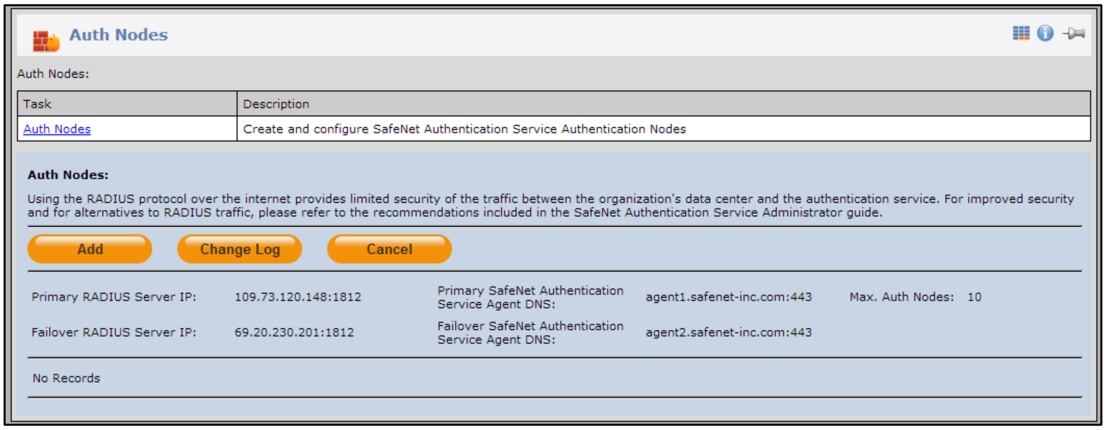
Service Start: 2013-07-17 Service Stop: 2016-02-05

Item	Capacity	KT	RB-1	MP-1/SMS	ICE MP-1/SMS	GRID	SecurID	OATH	SMS Credits	Password	RADIUS	GOLD	eToken	MobilePASS
Maximum	1	0	0	5	0	0	0	0	0	0	0	0	0	0
In Use	1	0	0	0	0	0	0	0	0	1	0	0	0	0

2. Click the **COMMS** tab, and then select **Auth Nodes**.



3. In the **Auth Nodes** module, click the **Auth Nodes** link.



Auth Nodes:

Task	Description
Auth Nodes	Create and configure SafeNet Authentication Service Authentication Nodes

Auth Nodes:

Using the RADIUS protocol over the internet provides limited security of the traffic between the organization's data center and the authentication service. For improved security and for alternatives to RADIUS traffic, please refer to the recommendations included in the SafeNet Authentication Service Administrator guide.

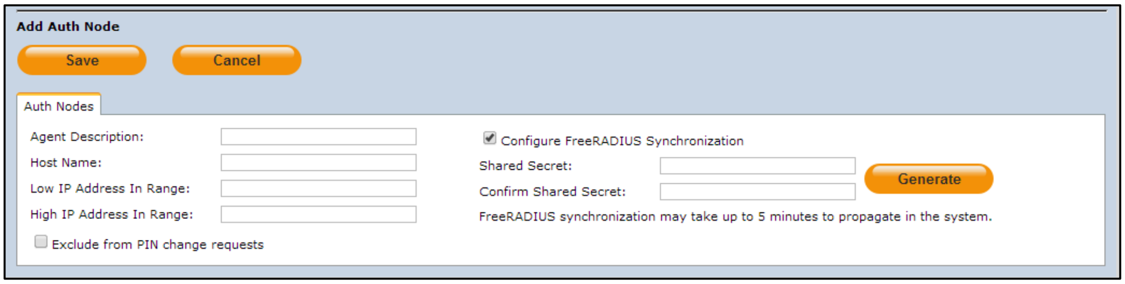
Primary RADIUS Server IP:	109.73.120.148:1812	Primary SafeNet Authentication Service Agent DNS:	agent1.safenet-inc.com:443	Max. Auth Nodes:	10
Failover RADIUS Server IP:	69.20.230.201:1812	Failover SafeNet Authentication Service Agent DNS:	agent2.safenet-inc.com:443		

No Records

4. Under **Auth Nodes**, click **Add**.

5. In the **Add Auth Nodes** section, complete the following fields, and then click **Save**:

Agent Description	Enter a host description.
Host Name	Enter the name of the host that will authenticate with SAS.
Low IP Address In Range	Enter the IP address of the host, or the lowest IP address in a range of addresses that will authenticate with SAS.
High IP Address In Range	Enter the highest IP address in a range of IP addresses that will authenticate with SAS.
Configure FreeRADIUS Synchronization	Select this option.
Shared Secret	Enter the shared secret key.
Confirm Shared Secret	Re-enter the shared secret key.



Add Auth Node

Agent Description:

Host Name:

Low IP Address In Range:

High IP Address In Range:

□ Exclude from PIN change requests

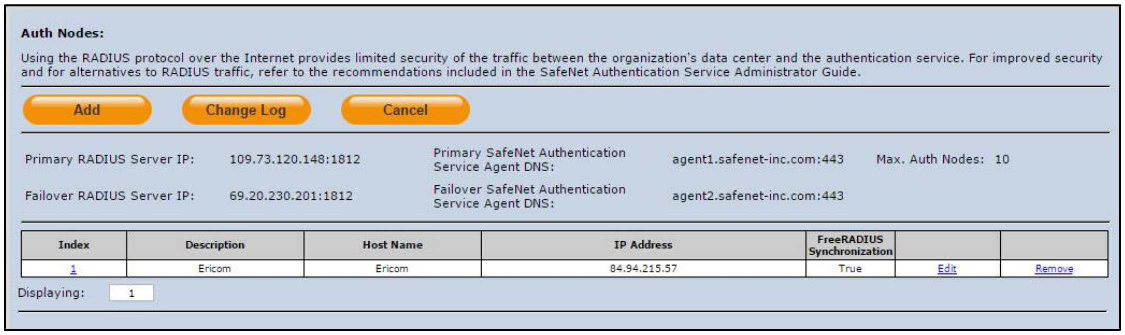
☑ Configure FreeRADIUS Synchronization

Shared Secret:

Confirm Shared Secret:

FreeRADIUS synchronization may take up to 5 minutes to propagate in the system.

The authentication node is added to the system.



Auth Nodes:

Using the RADIUS protocol over the Internet provides limited security of the traffic between the organization's data center and the authentication service. For improved security and for alternatives to RADIUS traffic, refer to the recommendations included in the SafeNet Authentication Service Administrator Guide.

Primary RADIUS Server IP: 109.73.120.148:1812

Primary SafeNet Authentication Service Agent DNS: agent1.safenet-inc.com:443

Max. Auth Nodes: 10

Failover RADIUS Server IP: 69.20.230.201:1812

Failover SafeNet Authentication Service Agent DNS: agent2.safenet-inc.com:443

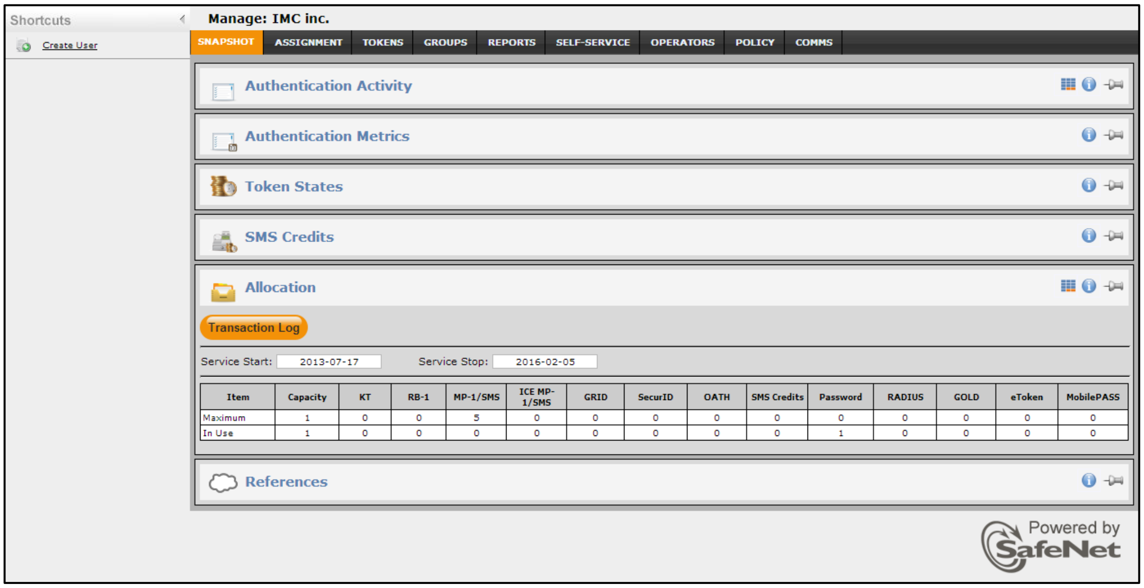
Index	Description	Host Name	IP Address	FreeRADIUS Synchronization		
1	Ericom	Ericom	84.94.215.57	True	Edit	Remove

Displaying: 1

Checking the SAS RADIUS Server’s IP Address

Before adding SAS as a RADIUS server in Ericom PowerTerm WebConnect, check the IP address. The IP address will then be added to Ericom PowerTerm WebConnect as a RADIUS server at a later stage.

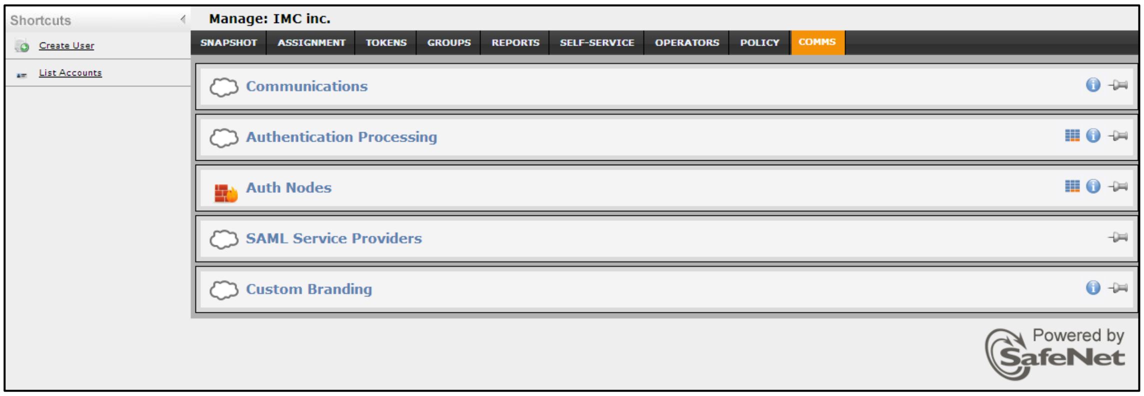
1. Log in to the SAS console with an Operator account.



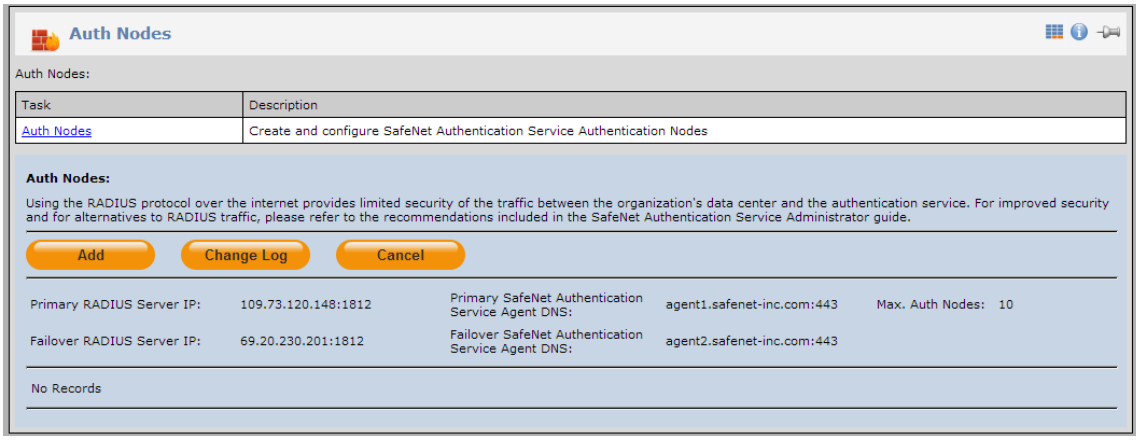
Service Start: 2013-07-17 Service Stop: 2016-02-05

Item	Capacity	KT	RB-1	MP-1/SMS	ICE MP-1/SMS	GRID	SecurID	OATH	SMS Credits	Password	RADIUS	GOLD	eToken	MobilePASS
Maximum	1	0	0	5	0	0	0	0	0	0	0	0	0	0
In Use	1	0	0	0	0	0	0	0	0	1	0	0	0	0

2. Click the **COMMS** tab, and then select **Auth Nodes**.



3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.



Auth Nodes:

Task	Description
Auth Nodes	Create and configure SafeNet Authentication Service Authentication Nodes

Auth Nodes:

Using the RADIUS protocol over the internet provides limited security of the traffic between the organization's data center and the authentication service. For improved security and for alternatives to RADIUS traffic, please refer to the recommendations included in the SafeNet Authentication Service Administrator guide.

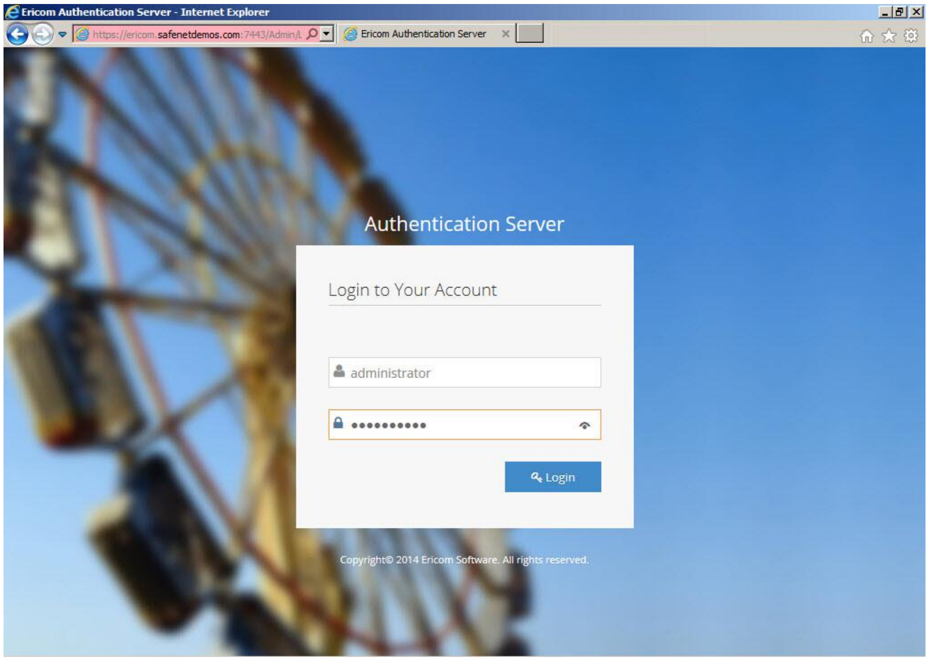
Primary RADIUS Server IP:	109.73.120.148:1812	Primary SafeNet Authentication Service Agent DNS:	agent1.safenet-inc.com:443	Max. Auth Nodes:	10
Failover RADIUS Server IP:	69.20.230.201:1812	Failover SafeNet Authentication Service Agent DNS:	agent2.safenet-inc.com:443		

No Records

Configuring Ericom PowerTerm WebConnect

The configuration of the Ericom PowerTerm WebConnect environment to work with RADIUS protocol is done through the Ericom Authentication Server Admin Console.

1. In a web browser, open the Ericom Authentication Server admin console URL: **http://<ViewServer>:7443/admin/login.html**
2. On the login page, enter your account credentials, and then click **Login**.


Ericom Authentication Server - Internet Explorer
https://ericom.safenetdemos.com:7443/Admin/L
Ericom Authentication Server
Authentication Server
Login to Your Account
Login

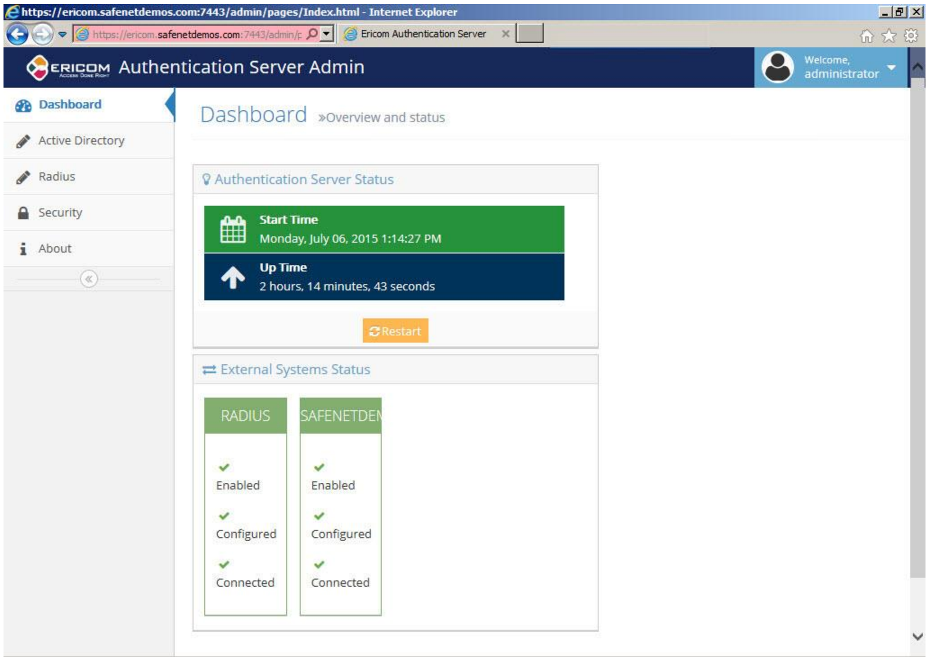
administrator

••••••••••

Copyright© 2014 Ericom Software. All rights reserved.

(The screen image above is from Ericom®. Trademarks are the property of their respective owners.)

3. In the left pane, click **Radius**.


https://ericom.safenetdemos.com:7443/admin/pages/Index.html - Internet Explorer
https://ericom.safenetdemos.com:7443/admin/p
Ericom Authentication Server
ERICOM
Authentication Server Admin
Welcome, administrator
Dashboard
Active Directory
Radius
Security
About
Dashboard »Overview and status
Authentication Server Status
Restart
External Systems Status

Start Time
Monday, July 06, 2015 1:14:27 PM

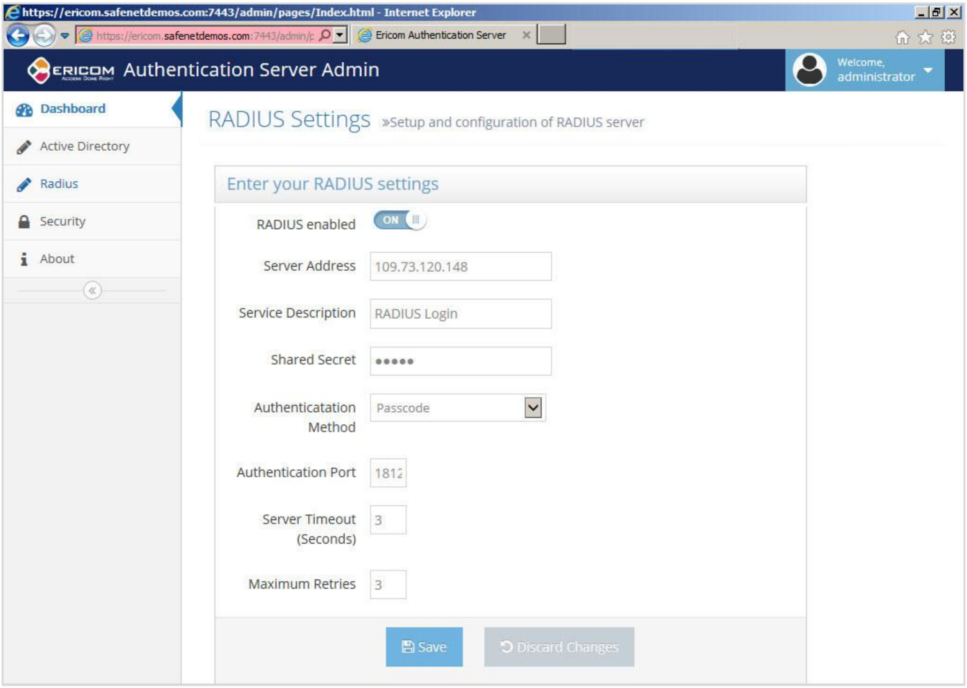
Up Time
2 hours, 14 minutes, 43 seconds

RADIUS	SAFENETDEM
✓ Enabled	✓ Enabled
✓ Configured	✓ Configured
✓ Connected	✓ Connected

(The screen image above is from Ericom®. Trademarks are the property of their respective owners.)

4. In the **RADIUS Settings** window, complete the following fields, and then click **Save**:

RADIUS enabled	Click **ON**.
Server Address	Enter the IAS/NPS server IP or hostname (for example, **109.73.120.148**).
Service Description	This is the RADUIS login’s headline. You can retain the default setting (**RADIUS Login**) or change it.
Shared Secret	Enter the RADIUS shared secret key.
Authentication Method	Select **Passcode**.
Authentication Port	Enter **1812**.
Server Timeout	Retain the default setting.
Maximum Retries	Retain the default setting.


https://ericom.safenetdemos.com:7443/admin/pages/Index.html - Internet Explorer
https://ericom.safenetdemos.com:7443/admin/p
Ericom Authentication Server
ERICOM Authentication Server Admin
Welcome, administrator
Dashboard
Active Directory
Radius
Security
About
Save
Discard Changes

RADIUS Settings »Setup and configuration of RADIUS server

Enter your RADIUS settings

RADIUS enabled: ON
Server Address: 109.73.120.148
Service Description: RADIUS Login
Shared Secret: ●●●●●
Authenticatation Method: Passcode
Authentication Port: 1812
Server Timeout (Seconds): 3
Maximum Retries: 3

(The screen image above is from Ericom®. Trademarks are the property of their respective owners.)

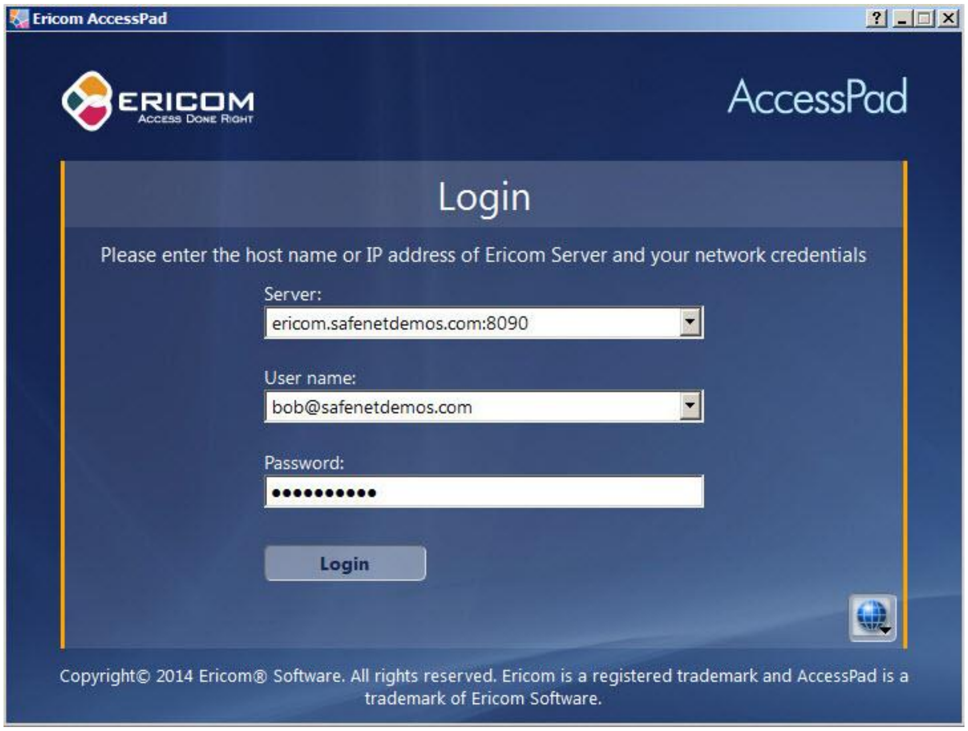
Running the Solution

These solutions describe how to connect to the Ericom PowerTerm WebConnect environment through either AccessPad or AccessPortal.

Signing in Through AccessPad

AccessPad is Ericom's rich client interface with local desktop integration, which allows users to connect to their Ericom PowerTerm WebConnect.

1. Launch the Ericom AccessPad client.
2. On the **Login** page, select the server to connect to your Ericom PowerTerm WebConnect environment, enter your organizational user name and password, and then click **Login**.



Please enter the host name or IP address of Ericom Server and your network credentials

Server: ericom.safenetdemos.com:8090

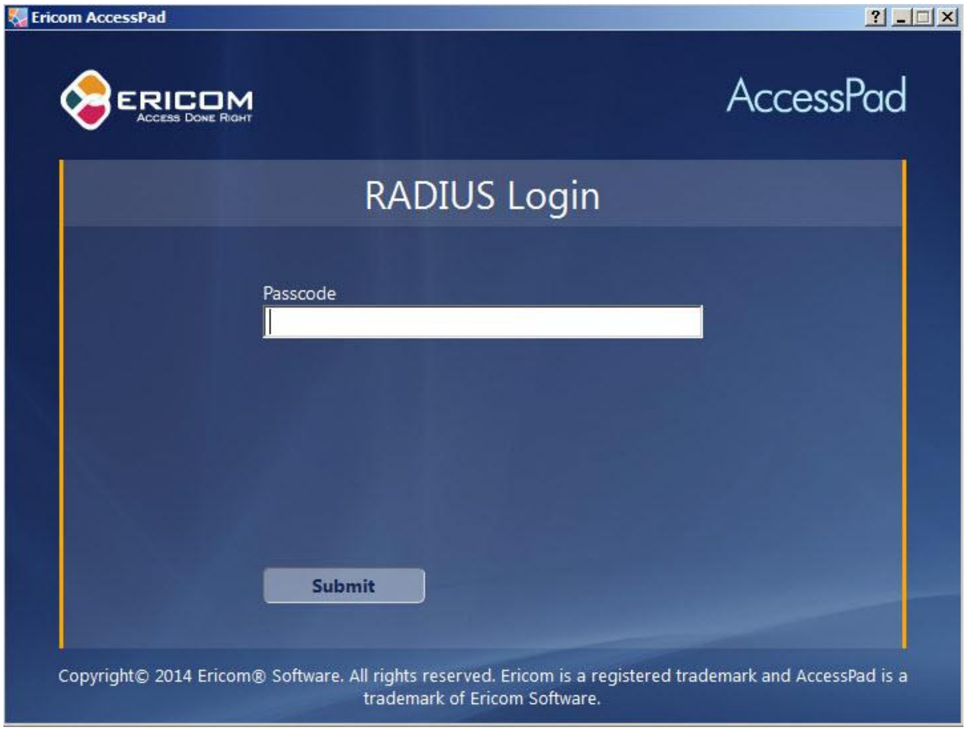
User name: bob@safenetdemos.com

Password: ••••••••••

Copyright© 2014 Ericom® Software. All rights reserved. Ericom is a registered trademark and AccessPad is a trademark of Ericom Software.

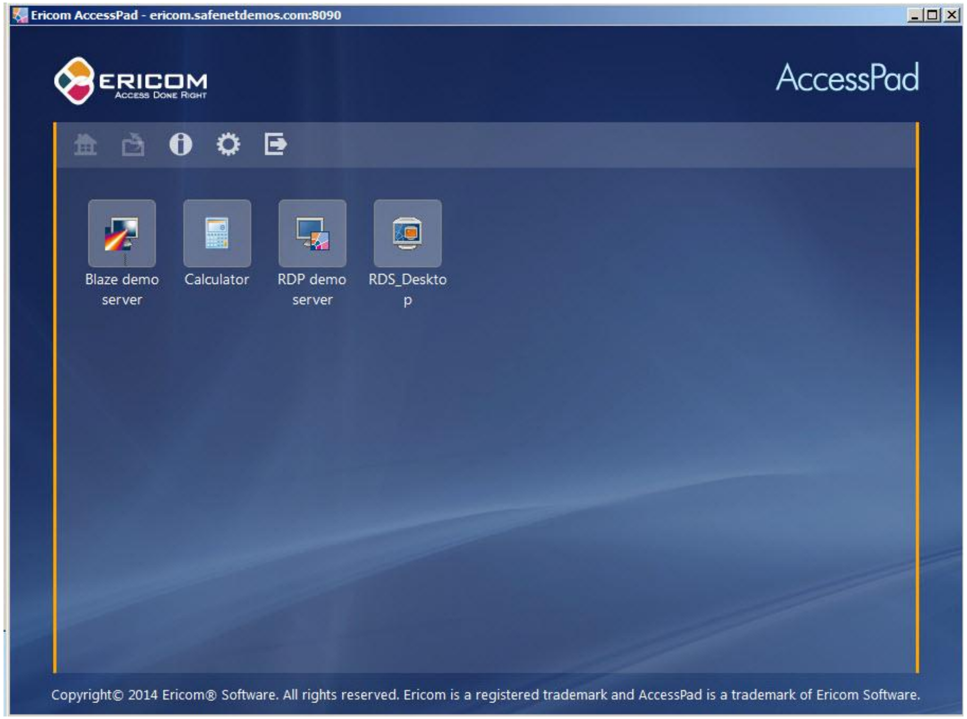
(The screen image above is from Ericom®. Trademarks are the property of their respective owners.)

3. On the **RADIUS Login** page, enter your SAS token (passcode), and then click **Submit**.


Ericom AccessPad
ERICOM
ACCESS DONE RIGHT
AccessPad
RADIUS Login
Passcode
Submit
Copyright© 2014 Ericom® Software. All rights reserved. Ericom is a registered trademark and AccessPad is a trademark of Ericom Software.

(The screen image above is from Ericom®. Trademarks are the property of their respective owners.)

4. After a successful authentication, you are connected to your PowerTerm WebConnect environment.

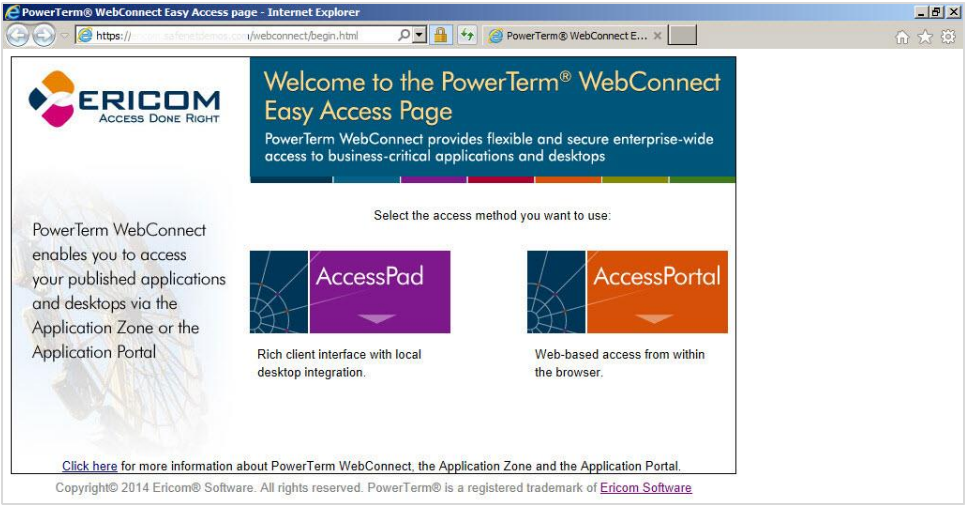

Ericom AccessPad - ericom.safenetdemos.com:8090
ERICOM
ACCESS DONE RIGHT
AccessPad
Blaze demo server
Calculator
RDP demo server
RDS_Deskto p
Copyright© 2014 Ericom® Software. All rights reserved. Ericom is a registered trademark and AccessPad is a trademark of Ericom Software.

(The screen image above is from Ericom®. Trademarks are the property of their respective owners.)

Signing in Through AccessPortal

AccessPortal is Ericom's web-based access from within the browser, which allows users to connect to their Ericom PowerTerm WebConnect.

1. Browse to the Ericom PowerTerm WebConnect portal URL (for example, **https://<Ericom_WebConnect_server>/WebConnect/begin.html**), and select **AccessPortal**.


PowerTerm® WebConnect Easy Access page - Internet Explorer
https:// safenetdemos.com/webconnect/begin.html
PowerTerm® WebConnect E...
ERICOM
ACCESS DONE RIGHT
AccessPad
AccessPortal

Welcome to the PowerTerm® WebConnect Easy Access Page

PowerTerm WebConnect provides flexible and secure enterprise-wide access to business-critical applications and desktops

Select the access method you want to use:

PowerTerm WebConnect enables you to access your published applications and desktops via the Application Zone or the Application Portal

Rich client interface with local desktop integration.

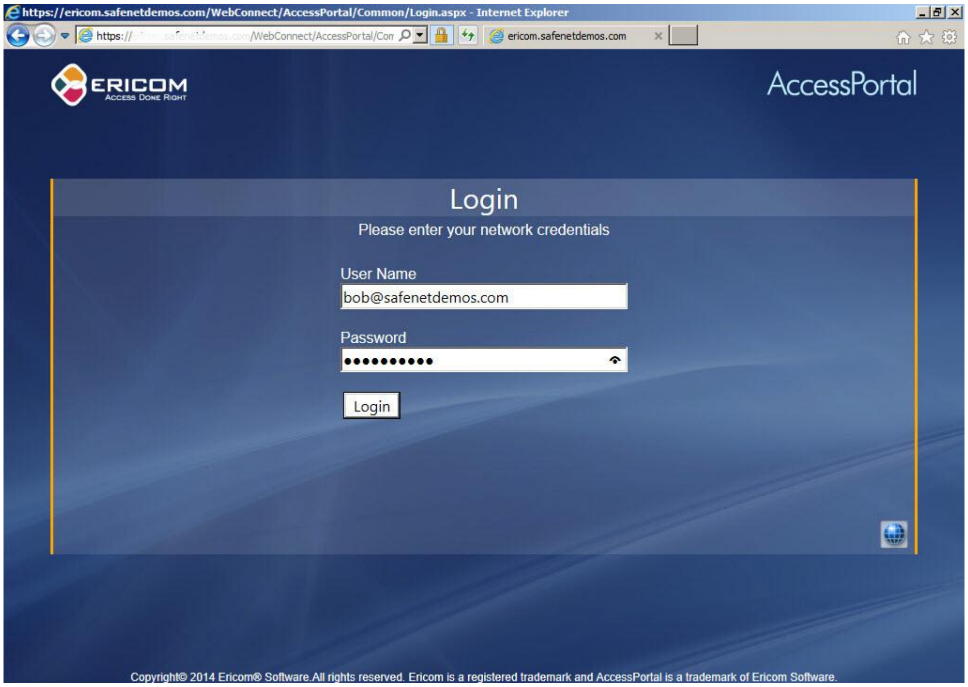
Web-based access from within the browser.

Click here for more information about PowerTerm WebConnect, the Application Zone and the Application Portal.

Copyright© 2014 Ericom® Software. All rights reserved. PowerTerm® is a registered trademark of Ericom Software

(The screen image above is from Ericom®. Trademarks are the property of their respective owners.)

2. On the **Login** page, enter your organizational user name and password, and then click **Login**.


https://ericom.safenetdemos.com/WebConnect/AccessPortal/Common/Login.aspx - Internet Explorer
https:// safenetdemos.com/WebConnect/AccessPortal/Com
ericom.safenetdemos.com
ERICOM
ACCESS DONE RIGHT
AccessPortal
Login

Login

Please enter your network credentials

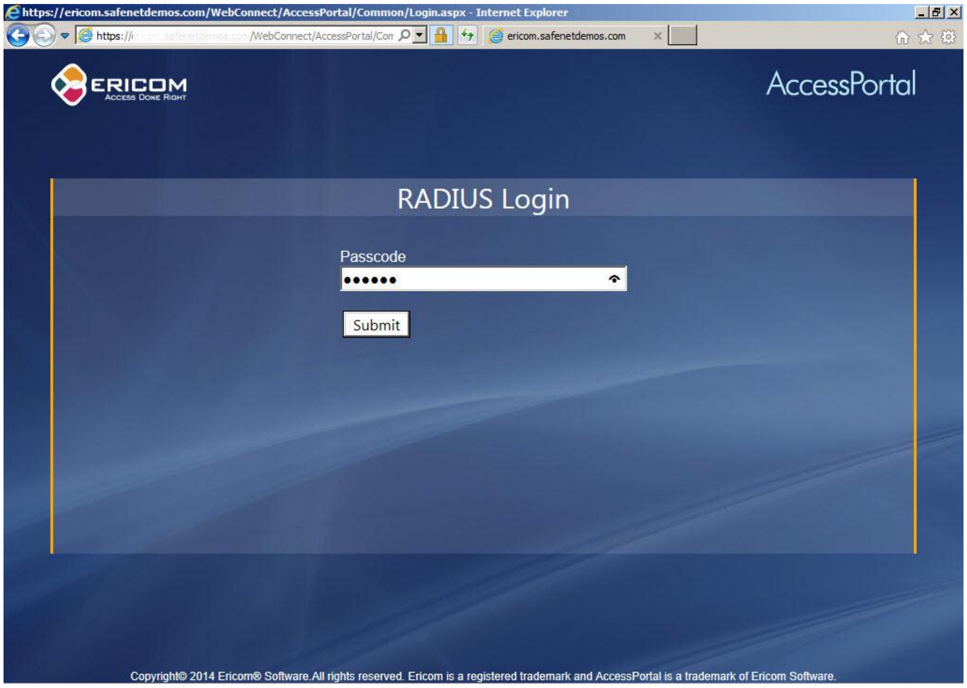
User Name: bob@safenetdemos.com

Password: ••••••••••

Copyright© 2014 Ericom® Software.All rights reserved. Ericom is a registered trademark and AccessPortal is a trademark of Ericom Software.

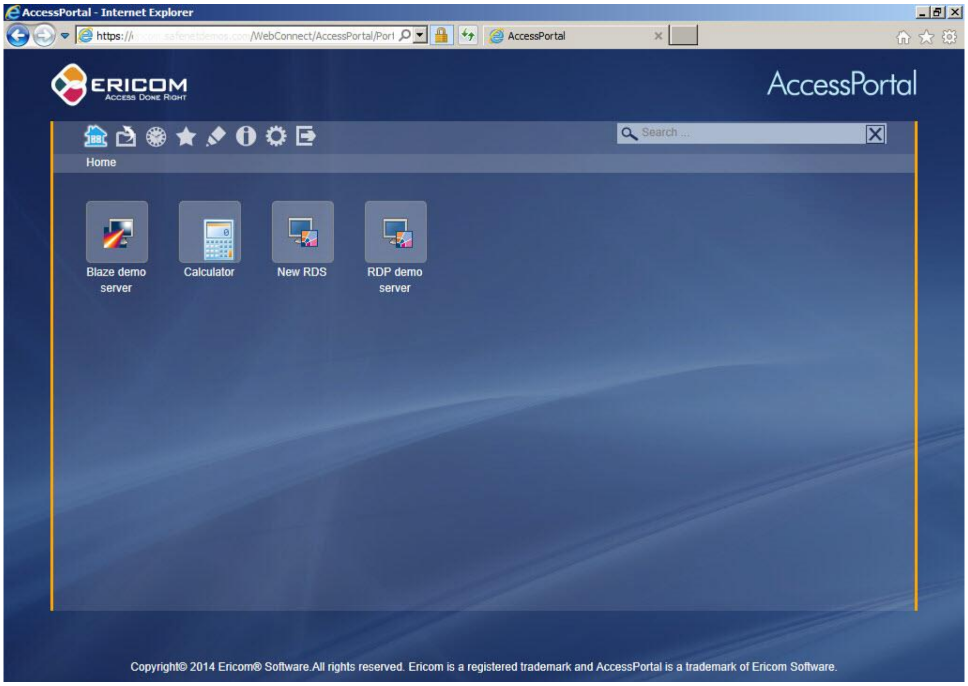
(The screen image above is from Ericom®. Trademarks are the property of their respective owners.)

3. On the **RADIUS Login** page, enter your SAS token (passcode), and then click **Submit**.


https://ericom.safenetdemos.com/WebConnect/AccessPortal/Common/Login.aspx - Internet Explorer
https://
/WebConnect/AccessPortal/Con
ericom.safenetdemos.com
ERICOM
Access Done Right
AccessPortal
RADIUS Login
Passcode
••••••
Submit
Copyright© 2014 Ericom® Software.All rights reserved. Ericom is a registered trademark and AccessPortal is a trademark of Ericom Software.

(The screen image above is from Ericom®. Trademarks are the property of their respective owners.)

4. After a successful authentication, you are connected to your PowerTerm WebConnect environment.


AccessPortal - Internet Explorer
https://
/WebConnect/AccessPortal/Port
AccessPortal
ERICOM
Access Done Right
AccessPortal
Search ...
Home
Blaze demo server
Calculator
New RDS
RDP demo server
Copyright© 2014 Ericom® Software.All rights reserved. Ericom is a registered trademark and AccessPortal is a trademark of Ericom Software.

(The screen image above is from Ericom®. Trademarks are the property of their respective owners.)

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 Gemalto Customer Support. Gemalto 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 Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	**Contact Information**	
Address	Gemalto, 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 Gemalto Knowledge Base.	