SafeNet Authentication Manager

Integration Guide

Using RADIUS Protocol for Ericom PowerTerm WebConnect

gemalto
security to be free

Document Part Number: 007-013266-001, 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 Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

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) tokens managed by SafeNet Authentication Manager.
- Configure Ericom PowerTerm WebConnect to work with SafeNet Authentication Manager 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 Manager and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on SafeNet Authentication Manager installation modes, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

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

Applicability

The information in this document applies to:

- **SafeNet Authentication Manager**—A server version of SAM 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 Manager**—Version 8.2 (HF 493)
- **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

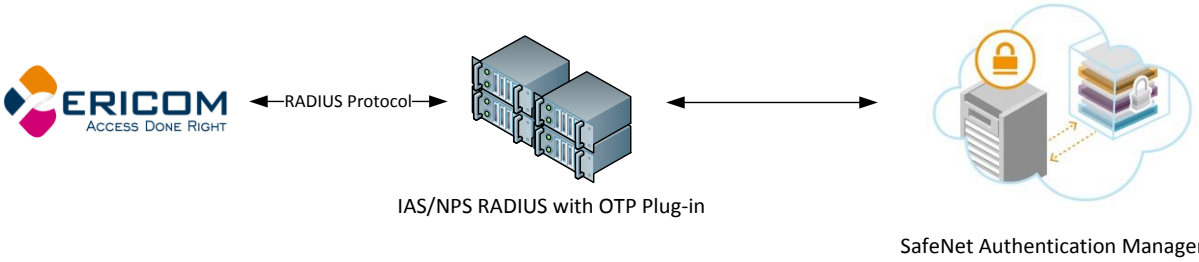
This document is targeted to system administrators who are familiar with Ericom PowerTerm WebConnect, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Manager.

RADIUS-based Authentication using SAM

SafeNet's OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SAM.

SAM's OTP plug-in for Microsoft RADIUS Client works with Microsoft's IAS or NPS, providing strong authenticated remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

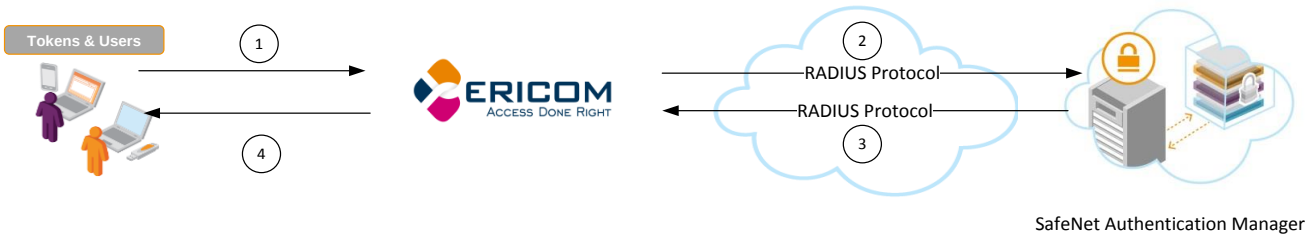


For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to the *SafeNet Authentication Manager 8.2 Administrator`s Guide*.

RADIUS Authentication Flow using SAM

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

The image below describes the dataflow 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 Manager for validation.
3. The SAM 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 SAM and his organization's Active Directory.

RADIUS Prerequisites

To enable SafeNet Authentication Manager 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 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 the RADIUS client for encryption, decryption, and digital signatures.

Configuring SafeNet Authentication Manager

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

Synchronizing Users Stores to SAM

SAM manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal ("stand-alone") user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Microsoft Active Directory 2003, 2008, and 2008 R2
- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

Configuring SAM's Connector for OTP Authentication

SafeNet Authentication Manager is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications, including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected the **Simplified OTP-only** configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The **Simplified OTP-only** configuration is as follows:

- **Connectors**—SAM Connector for OTP Authentication is installed
- **SAM Back-end Service**—Activated on this server; scheduled to operate every 24 hours

In addition, the SAM default policy is set as follows:

- OTP support (required for OTP) is selected in the **Token Initialization** settings.
- The **SAM Connector for OTP Authentication** is set, by default, to enable enrollment of OTP tokens without requiring changes in the Token Policy Object (TPO) settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide*.

Assigning a Token in SAM

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

The following tokens are supported:

- eToken PASS
- eToken NG-OTP
- SafeNet GOLD
- SMS tokens
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)
- SafeNet eToken 3400
- SafeNet eToken 3500

Tokens can be assigned to users as follows:

- **SAM Management Center**—Management site used by SAM administrators and help desk personnel for token enrollment and lifecycle management.
- **SAM Self-Service Center**—Self-service site used by end users for managing their tokens.
- **SAM Remote Service**—Self-service site used by employees not on the organization's premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet's tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide*.

Adding Ericom PowerTerm WebConnect as a RADIUS Client in IAS/NPS

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in Ericom PowerTerm WebConnect.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in Ericom PowerTerm WebConnect.

Ericom PowerTerm WebConnect must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize Ericom PowerTerm WebConnect for authentication.

NOTE: This document assumes that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

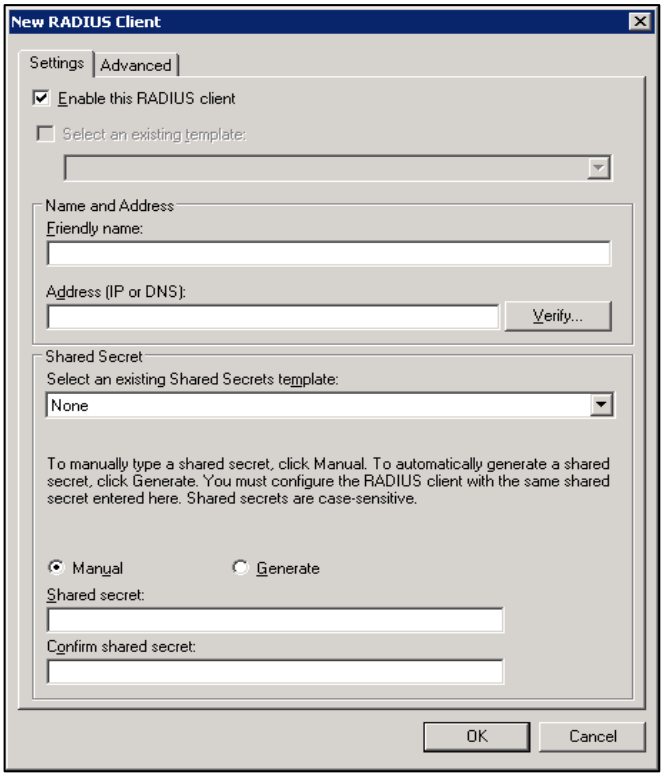
The details below refer to NPS, and are very similar to IAS.

1. Click **Start > Administrative Tools > Network Policy Server**.
2. From the NPS web console, in the left pane, expand **RADIUS Clients and Servers**, right-click **RADIUS Clients** and then click **New**.

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

3. On the **New RADIUS Client** window, complete the following fields on the **Settings** tab:

Enable this RADIUS client	Select this option.
Friendly name	Enter a RADIUS client name.
Address (IP or DNS)	Enter the Ericom PowerTerm WebConnect IP address or DNS.
Manual/Generate	Select **Manual**.
Shared secret	Enter the shared secret for the RADIUS client. This entry must match the shared secret that was used when the RADIUS server was configured in Ericom PowerTerm WebConnect.
Confirm shared secret	Re-enter the shared secret.



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

4. Click **OK**. Ericom PowerTerm WebConnect is added as a RADIUS client in NPS.

Configuring SAM's OTP Plug-In for Microsoft RADIUS Client

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) as Windows services running a RADIUS server. These services may be extended by adding plug-ins for the authentication process.

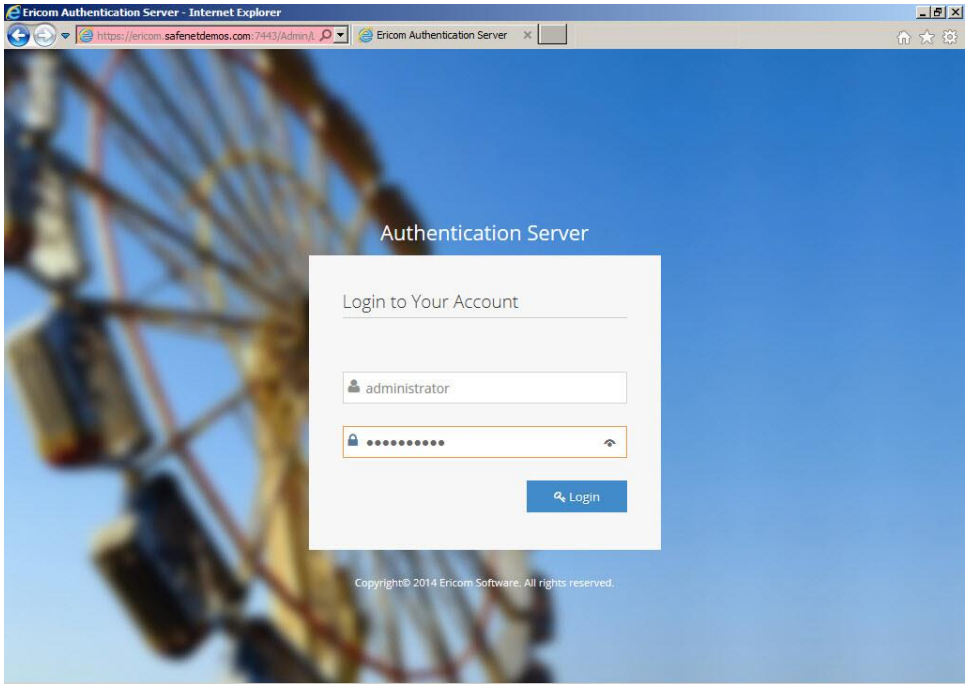
SAM's OTP plug-in for Microsoft RADIUS Client works with Microsoft's IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP plug-in, refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide*.

Configuring Ericom PowerTerm WebConnect

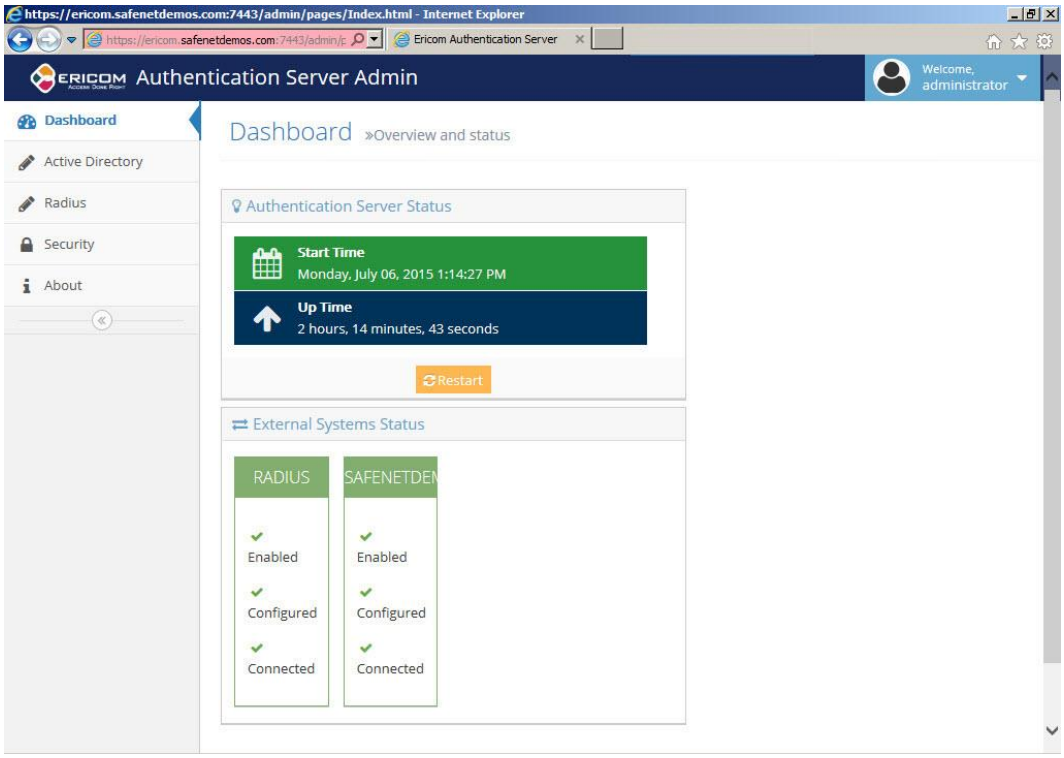
The configuration of Ericom PowerTerm WebConnect environment to work with RADIUS protocol is done through the Ericom Authenticaiton Server Admin Console.

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**.



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

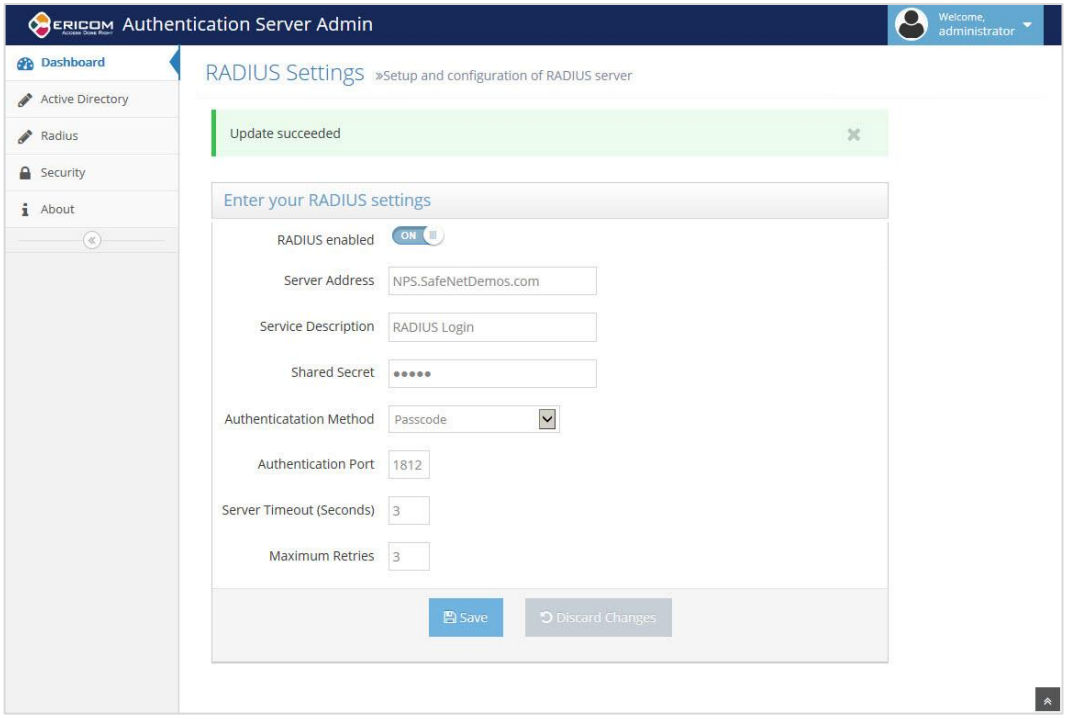
3. In the left pane, click **Radius**.



(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, **NPS.SafeNetDemos.com**).
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.



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

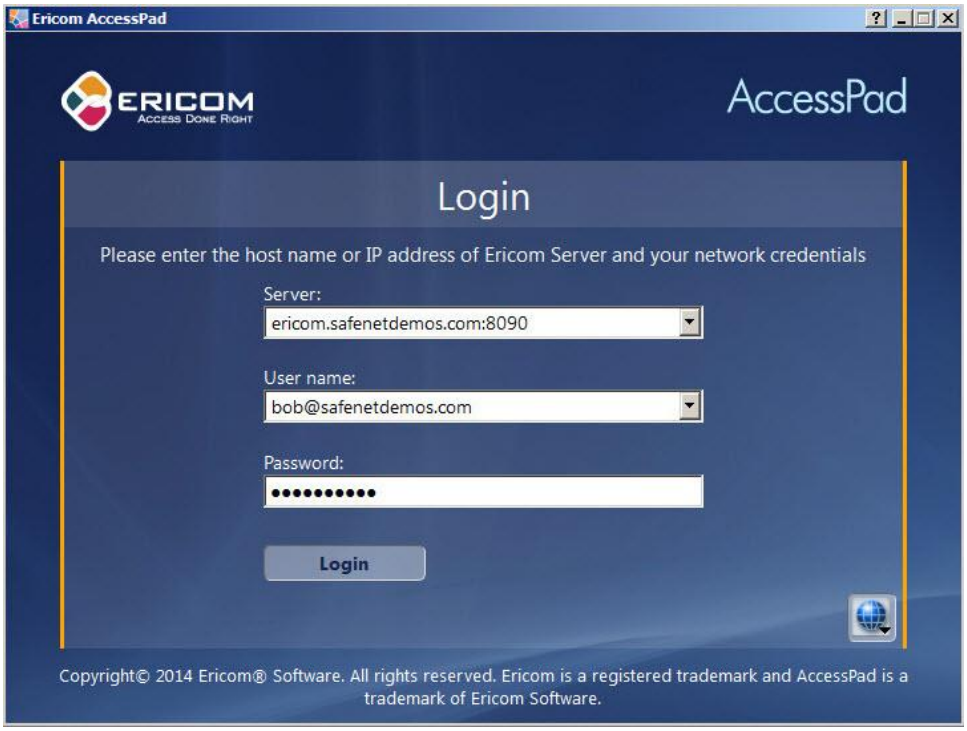
Running the Solution

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

Sign in Through AccessPad

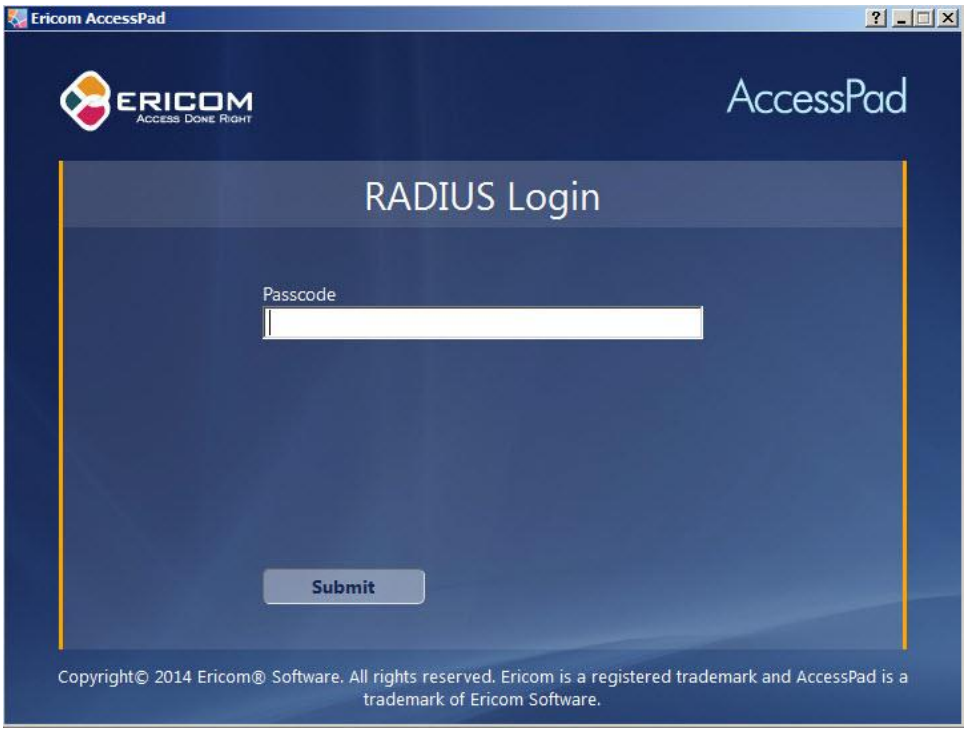
AccessPad is Ericom's rich client interface with local desktop integration, which allows users to connect to their Ericom PowerTerm WebConnect.

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.**



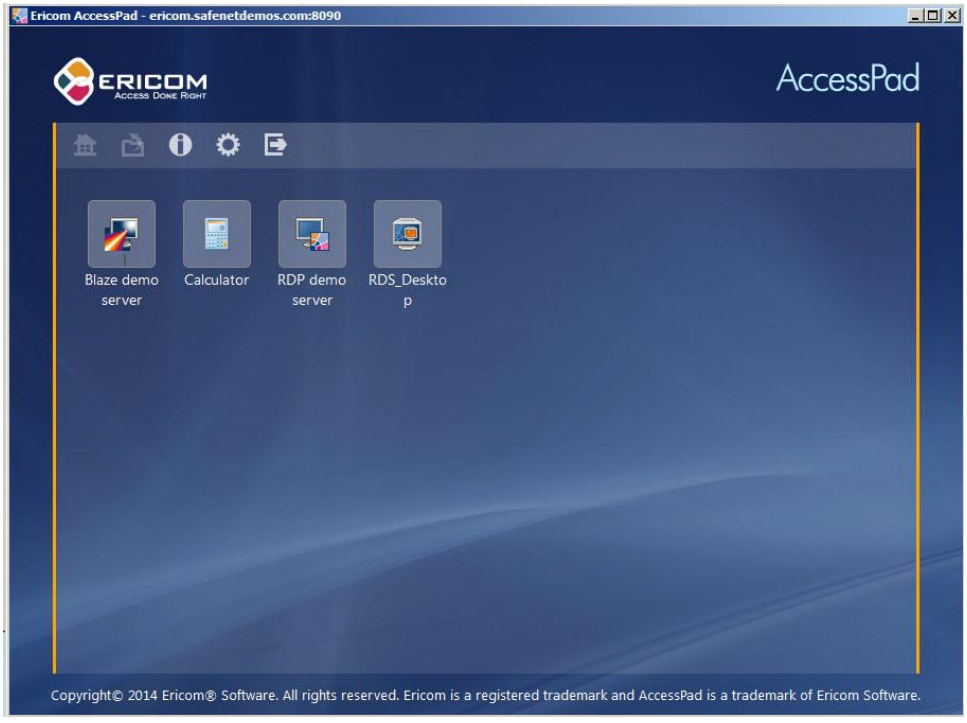
(The screen image above is from Ericom®. Trademarks are the property of their respective owners.)

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



(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.

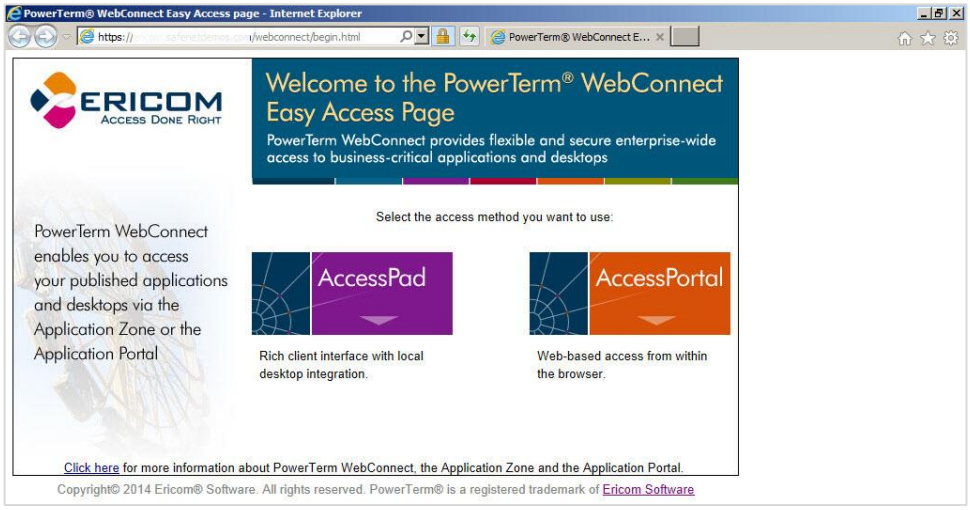


(The screen image above is from Ericom®. Trademarks are the property of their respective owners.)

Sign in Through AccessPortal

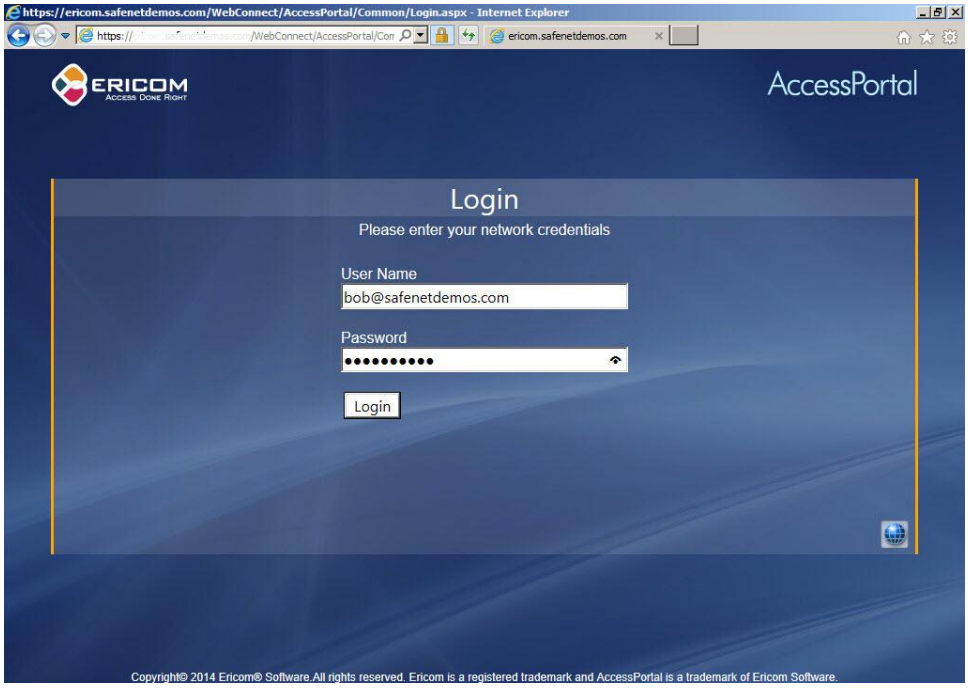
AccessPortal is Ericom's web-based access from within the browser, which allows users to connect to their Ericom PowerTerm WebConnect.

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



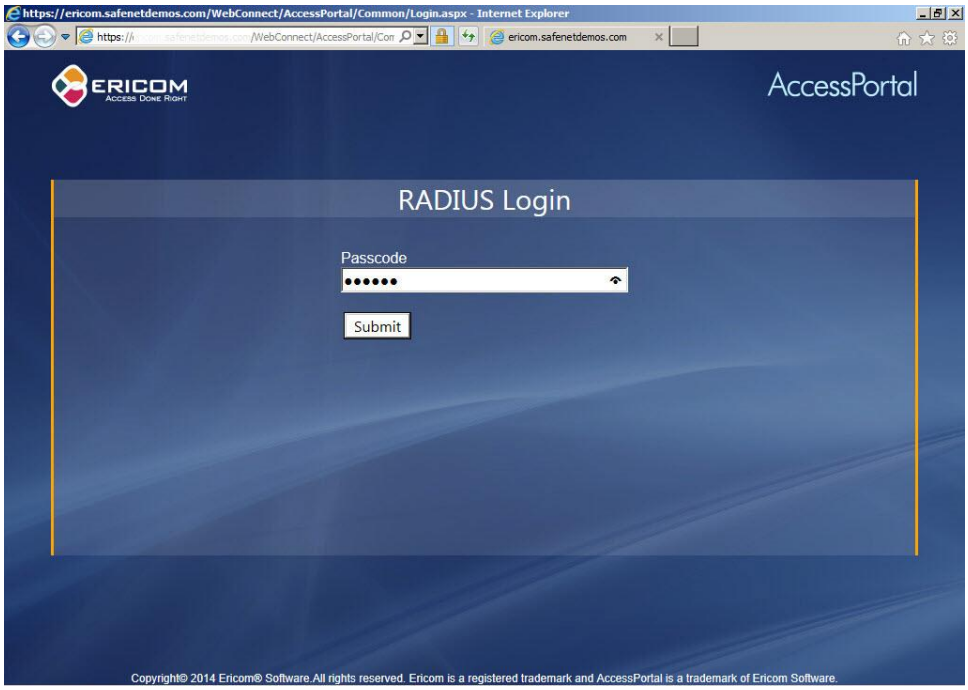
(The screen image above is from Ericom®. Trademarks are the property of their respective owners.)

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



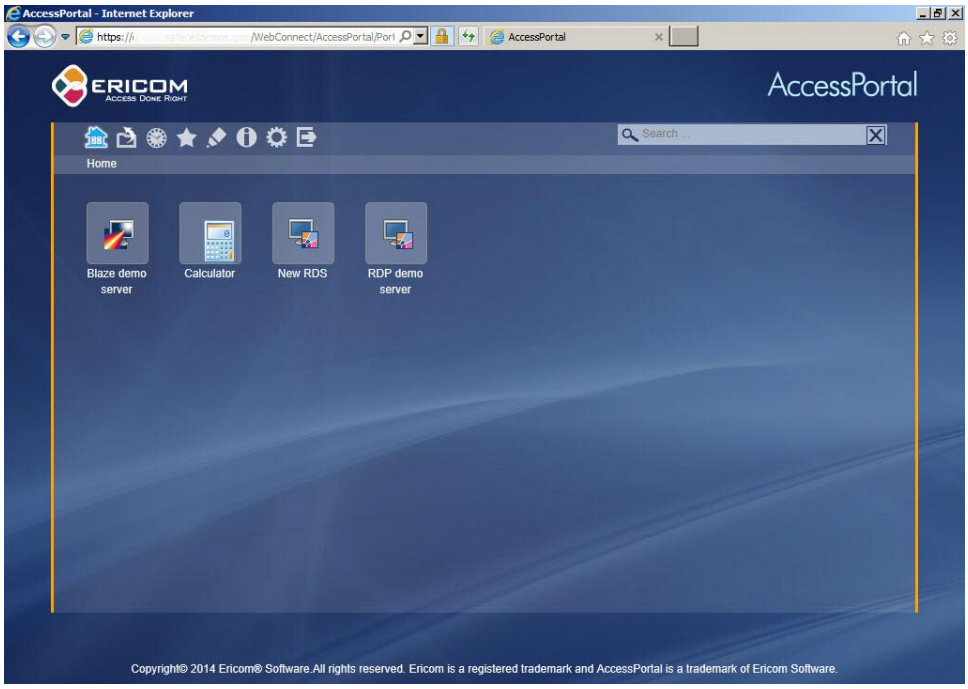
(The screen image above is from Ericom®. Trademarks are the property of their respective owners.)

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



(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.



(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.	