Two-factor Authentication: A Tokenless Approach

Multi-factor Authentication Layer

Tech Brief

v.3.2-014
# PortalGuard Two-factor Authentication: A Tokenless Approach

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>2</td>
</tr>
<tr>
<td>The Basics</td>
<td>2</td>
</tr>
<tr>
<td>One-time Passwords - PortalGuard Options</td>
<td>2</td>
</tr>
<tr>
<td>OTP Delivery Methods</td>
<td>3</td>
</tr>
<tr>
<td>Benefits</td>
<td>3</td>
</tr>
<tr>
<td>Beyond Two-factor Authentication</td>
<td>4</td>
</tr>
<tr>
<td>Why PortalGuard?</td>
<td>4</td>
</tr>
<tr>
<td>How it Works</td>
<td>4</td>
</tr>
<tr>
<td>User Enrollment</td>
<td>4</td>
</tr>
<tr>
<td>Two-factor Authentication Process</td>
<td>5</td>
</tr>
<tr>
<td>Login Directly to a Cloud/Web-based Application</td>
<td>5</td>
</tr>
<tr>
<td>Login via a SSL VPN Using RADIUS</td>
<td>8</td>
</tr>
<tr>
<td>OTP Configurations</td>
<td>11</td>
</tr>
<tr>
<td>Deployment</td>
<td>12</td>
</tr>
<tr>
<td>IIS Installation</td>
<td>12</td>
</tr>
<tr>
<td>System Requirements</td>
<td>13</td>
</tr>
<tr>
<td>Platform Layers</td>
<td>13</td>
</tr>
<tr>
<td>Appendix</td>
<td>15</td>
</tr>
<tr>
<td>A: SMS OTP Delivery Method</td>
<td>15</td>
</tr>
<tr>
<td>B: Voice OTP Delivery Methods</td>
<td>16</td>
</tr>
<tr>
<td>C: Hardware Token OTP Delivery Method</td>
<td>18</td>
</tr>
<tr>
<td>D: Transparent Tokenless Toolbar for TOTP Delivery Method</td>
<td>19</td>
</tr>
<tr>
<td>E: Printed OTP Delivery Method</td>
<td>21</td>
</tr>
</tbody>
</table>
Summary

PortalGuard is a software solution designed as a strong authentication platform, consisting of five layers including two-factor authentication, single sign-on, self-service password management, contextual authentication, and password synchronization, used for protecting browser-based applications which are hosted within an Intranet and/or outside the firewall, now commonly known as the Cloud.

These applications contain functionality to read, edit and search data at all levels of sensitivity, across multiple industries. The access point for browser-based applications is the login screen where you are typically required to prove your identity by providing a username and password. This is normally sufficient to prove you are authorized and therefore granted access to company applications and data.

Although still used as an integral part of authentication, passwords alone are inadequate for today’s browser-based applications. They are easily exploited by unauthorized users who find new methods of stealing passwords and impersonating authorized users. With that said, the true purpose of this document is to describe alternatives to using passwords.

Many choices in the market strengthen your authentication, to prevent unauthorized access, by providing two-factor authentication. Two-factor is an acceptable way to increase security; however, inflexibility and low usability have proven to be barriers for many organizations with the primary barrier being high total cost of ownership in today’s economic climate. Token-based approaches are expensive and problematic when hardware is forgotten, needs repair or replacement. PortalGuard avoids these barriers by providing a flexible and cost-effective approach which is easily accepted by users.

The Basics

Two-factor authentication is used to increase security by requiring you to provide “something you know” (a password) and leverage “something you have” (laptop, mobile phone). The use of two distinct authentication factors helps eliminate an organization’s security concerns around granting access based on a single, knowledge-based factor.

One-time Passwords - PortalGuard Options

Increasing in popularity, a one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings with static passwords, including being unsusceptible to replay attacks. If a potential intruder manages to record an OTP that was already used to log into a server, he or she will not be able to reuse it since it will no longer be valid.

The traditional method of delivering an OTP via a hard token or key fob has fallen out of favor due to cost and usability issues. Use of “soft tokens”, like mobile phones, has supplanted it.

PortalGuard can enforce two-factor authentication and deliver an OTP when the user is trying to access the web/cloud application directly, through an VPN connection using RADIUS, or when performing a self-service password reset, recovery, or account unlock.

PortalGuard not only leverages the user’s mobile device, but with its unique offering of transparent tokens, leverages the user’s laptop as well. A transparent token can be made up of several different types of parameters, including a random number, device serial numbers and/or Active Directory identifiers.
Together these will make up the OTP which is then encrypted and passed from the client machine to the PortalGuard server.

### OTP Delivery Methods:

<table>
<thead>
<tr>
<th>Method</th>
<th>Initial Cost</th>
<th>Device Cost</th>
<th>Required Support</th>
<th>Client Software</th>
<th>Cost Per Transaction</th>
<th>Ease of Use</th>
<th>Portability</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS</td>
<td>Low</td>
<td>Low</td>
<td>None</td>
<td>Low</td>
<td>No</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Transparent Tokenless Toolbar</td>
<td>Low</td>
<td>High</td>
<td>None</td>
<td>Low</td>
<td>Yes</td>
<td>None</td>
<td>High</td>
</tr>
<tr>
<td>Email</td>
<td>Low</td>
<td>Low</td>
<td>None</td>
<td>Low</td>
<td>No</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Printer*</td>
<td>Low</td>
<td>Low</td>
<td>None</td>
<td>Low</td>
<td>No</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Hardware Token</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>No</td>
<td>None</td>
<td>Medium</td>
</tr>
<tr>
<td>Landline (wav file)</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>None</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>

* MITM - Man-in-the-Middle Attack

<table>
<thead>
<tr>
<th>Attack Prevention</th>
<th>Passive*</th>
<th>Active*</th>
<th>MITM*</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Transparent Tokenless Toolbar</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Email</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Printer*</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Hardware Token</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Landline (wav file)</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

With PortalGuard you can deliver an OTP via SMS, hosted text-to-speech, SIP, email, printer or transparent token to achieve two-factor authentication. Please view appendices A-E for information on the individual delivery methods.

### Benefits

- Increased security - add an extra layer of authentication to application access, VPN access, or during a self-service password reset
- Reduce Risk - prevent attacks by leveraging credentials which expire after one use
- Usability - leverage hardware a user already has for increased user adoption
- Eliminate forgotten passwords - leverage a username and OTP only as credentials
- Configurable - to the user, group or application levels
- Flexible - multiple OTP delivery methods available
Beyond Two-factor Authentication

PortalGuard’s flexibility allows you to choose the appropriate authentication method for each user, group or application, by leveraging Contextual Authentication. Varying access scenarios in every organization drive the need for this type of authentication. For instance, users within your company’s four walls may only need to provide strong passwords whereas a traveling salesperson or roaming user is presented with two-factor authentication.

However, a traveling salesperson now in the office only needs to provide a password to prove his identity due to his new situation when requesting access. Contextual Authentication is a solution with the flexibility to match your individual users’ needs and organizational goals.

Why PortalGuard?

- Flexible authentication platform which expands with you and your requirements
- Low total cost of ownership
- Configurable – apply the appropriate authentication method to the user, group or application
- Gain usage Insight – optionally collect location, time, device, network and application details for each access request
- No additional hardware – leverage devices users already use daily
- Easy installation and deployment
- Seamless integration with existing environment
- Developed/supported by authentication experts

How it Works

User Enrollment

Once two-factor authentication becomes a requirement, the user will be prompted to enroll their mobile phone. PortalGuard provides flexibility around this process by allowing you to configure whether the enrollment will be forced or able to be postponed “x” number of times by the user. This increases the usability for users, giving them options around a process many find intrusive and blocking.

Phone enrollment can also be automated by importing the data from any current corporate data source.
Two-factor Authentication Process - Login Directly to a Cloud/Web-based Application

The following process shows the two-factor authentication process when a user is logging in directly to a cloud/web-based application.

**Step 1:** PortalGuard’s login screen is presented when a user visits the web-application. This login screen can be fully customized to match your organization’s branding, creating a seamless experience for the user.

![PortalGuard Login Screen](image)

**Step 2:** The user enters their username and clicks “Continue”

![Username Entry](image)
Step 3: The PortalGuard server sends the OTP to the user’s mobile phone within 5-10 seconds, in the form of an SMS. NOTE: PortalGuard can send the OTP via SMS, email, printer or transparent token.

Step 4: The user is prompted for a password and OTP.
Step 5: The user enters in the OTP they received and clicks “Log On”

Step 6: The user gains access to the web-application and data.

Step 7: This is an example of a user attempting to use an expired OTP that was never used. Once the expired OTP is entered, the user is denied access and prompted to cancel the process or request a valid OTP. However if the user attempts to reuse a used OTP or an unauthorized user is attempting to perform a replay attack, PortalGuard will display a dialog showing "Incorrect OTP Provided" if strikeouts are disabled.
Two-factor Authentication Process - Login via a SSL VPN Using RADIUS:

The following steps show the two-factor authentication process when a user is logging into a cloud/web-based application via a SSL VPN connection using the RADIUS protocol.

**RADIUS Support**

RADIUS is a well-established, vendor-neutral network protocol which is an internet standard that was primarily designed to authenticate remote users for dial-up services and it is widely implemented by numerous network security vendors such as Cisco, Juniper, Citrix and Checkpoint.

Due to the widespread support for the RADIUS protocol by network security vendors, RADIUS is an optimal choice for enabling two-factor authentication for remote access users. In the standard case, a network security appliance, firewall or Network Access Server (NAS) is the “RADIUS client” or “NAS client” and the PortalGuard server acts as the “RADIUS server”. The end-user only communicates directly with the NAS client to provide the login information.

Because the NAS client communicates directly with the PortalGuard RADIUS server, authentication decisions made by PortalGuard are strictly enforced. This ensures a high level of security and consistency.

Most network security appliances allow VPN users to be authenticated using different mechanisms. A few common options are:

- User accounts defined locally on the appliance
- LDAP authentication
- X.509 certificates
- RADIUS

Enabling multi-factor authentication can be as straightforward as enabling RADIUS authentication on your network security appliance, pointing it to the PortalGuard server and adding a RADIUS client configuration in PortalGuard.

The same RADIUS setup can often be used to authenticate remote users looking for a SSL VPN via web browser -AND- remote users with VPN software installed locally on their workstation. This helps offer a high degree of consistency reducing the need for user training and education.

**How it Works**

**Step 1:** The user attempts to connect to the NAS/firewall using either a browser or VPN client software and is prompted for username and password.
Steps 2-5 happen transparently to the user:

**Step 2:** The NAS communicates the credentials to the PortalGuard server using the RADIUS protocol.

**Step 3:** The PortalGuard server validates the user's credentials against its configured user repository (e.g. Active Directory).

**Step 4:** The user repository returns a success or failure code indicating the fidelity of the username and password.

**Step 5:** PortalGuard replies to the RADIUS request with an *Access-Challenge* response that includes a custom message that should be displayed to the user and a random identifier (the "state") that the NAS will send back to PortalGuard to identify the same user session.

**Step 6:** The NAS displays the custom message requesting the user to enter the OTP that was sent to their mobile device.
Step 7: The user enters the OTP from their mobile device and submits it to the NAS.
Steps 8 and 9 happen transparently to the user:

**Step 8:** The NAS sends the OTP and state identifier to PortalGuard using RADIUS.

**Step 9:** The PortalGuard server replies to the RADIUS 2nd request with an Access-Accept response.

**Step 10:** The NAS accepts the user’s authentication and the VPN tunnel/session is established. The user is then able to access internal resources (e.g. “crm.acme.com”).

**OTP Configuration**

*NOTE: All the following settings are policy specific, so you can have different values for different users/groups/hierarchies.*

**Configurable through the PortalGuard Configuration Utility:**

- Expiration, aka “time-to-live” (TTL)
- Length
- Format
  - Numeric characters only
  - Upper/lowercase characters
  - Upper/lowercase & numeric characters
  - Upper/lowercase, numeric and symbol characters
• Delivery format, including From, Subject and Body Fields:

**Deployment**

Implementation of the PortalGuard platform is seamless and requires no changes to Active Directory/LDAP schema. A server-side software installation is required on each IIS server for which PortalGuard’s authentication functionality is desired. Additional client-side software is required for use of contextual authentication and/or transparent tokens.

**IIS Installation**

A MSI is used to install PortalGuard on IIS 6 or 7.x. If installing PortalGuard on IIS 7.x/Windows Server 2008, make sure to have installed the following feature roles prior to launching the MSI:

1. All the Web Server Management Tools role services
2. All the Application Development role services
3. All IIS 6 Management Compatibility role services

The MSI is a wizard-based install which will quickly guide you through the installation.
System Requirements

PortalGuard can be installed directly on the following web servers:

- IBM WebSphere/WebSphere Portal v5.1 or higher
- Microsoft IIS 6.0 or higher
- Microsoft Windows SharePoint Services 3.0 or higher
- Microsoft Office SharePoint Server 2007 or later

To support two-factor authentication to a VPN using RADIUS the following is required:

- The network appliance must support RADIUS as an authentication option.
- The network appliance must support the Access-Challenge response type as well as the State and Reply-Message attributes.
- PortalGuard must be licensed for RADIUS support.
- End-user enrollment of mobile devices or challenge answers must be performed external to the RADIUS protocol.

The PortalGuard Web server also has the following requirements on Windows operating systems:

- .NET 2.0 framework or later must be installed
- (64-bit OS only) Microsoft Visual C++ 2005 SP1 Redistributable Package (x64)

PortalGuard is fully supported for installation on virtual machines. Furthermore, PortalGuard can currently be installed on the following platforms:

- Microsoft Windows Server 2000
- Microsoft Windows Server 2003 (32 or 64-bit)
- Microsoft Windows Server 2008 (32 or 64-bit)
- Microsoft Windows Server 2008 R2

If you have a platform not listed here, please contact us at sales@portalguard.com to see if we have recently added support for your platform.

Platform Layers

Beyond two-factor authentication, PortalGuard is a flexible authentication platform with multiple layers of available functionality to help you achieve your authentication goals:

- Contextual Authentication
- Self-service Password Reset
- Real-time Reports / Alerts
- Knowledge-based
- Password Management
- Single Sign-on
Appendix A: SMS OTP Delivery Method

For SMS delivery, PortalGuard leverages telephone companies’ SMTP-to-SMS gateways. This is why PortalGuard asks for both the phone number and the provider. An SMTP-to-SMS gateway is a free service maintained by the telephone companies to allow an email sent via SMTP to be delivered to a user’s phone as a SMS/text message. The provider is needed to determine the gateway (e.g. "@txt.att.com" for AT&T) and can then build the full email address (phonenum@gateway). Leveraging these services allows PortalGuard to be deployed quickly (it only needs a SMTP relay for sending outbound emails as opposed to a modem and dedicated POTS line for full-blown SMS) and more cheaply (there is no cost incurred by the sender for each OTP sent nor does a phone line need to be maintained).

SMS Gateway Support
SMS OTPs delivered via mobile carrier’s email to SMS Gateway

1. Username/Password for Web Application Login
2. OTP sent to SMTP server
3. OTP sent via email to mobile carrier’s Email to SMS Gateway
4. User inputs OTP into required login field
Appendix B: Voice OTP Delivery Methods

PortalGuard can deliver a voice OTP, a text-to-speech WAV file, to a user’s landline phone using two methods, a hosted text-to-speech service or by leveraging the SIP protocol.

**Hosted Text-To-Speech**
A text-based template is configured by the customer in PortalGuard. An account is created by the customer directly with a third-party service provider (PortalGuard does not provide this service). PortalGuard connects to the third-party hosted service which converts the template with the user’s one-time passcode into a WAV file and places a phone call to the end-user’s enrolled phone (land line or mobile) and plays the WAV file. The service typically offers the user the option of pressing a key to repeat the voice message. Each call placed through the third-party service deducts credits from the customer’s account. Credits can typically be added at any time. The user types the OTP from the voice message into the PortalGuard browser interface to continue the authentication.
**SIP**

Session Initiation Protocol (SIP) is a standards-based, widely implemented protocol used for controlling communication sessions such as voice calls over Internet Protocol (IP). The SIP integration available through PortalGuard allows customers to leverage their own existing phone infrastructure to place the phone calls when delivering an OTP. This is typically a more cost-effective option than using a third-party hosted service provider. Similar to the Hosted text-to-speech option, a text-based template is configured by the customer in PortalGuard and the OTP is substituted into it at runtime. PortalGuard then converts the text to a WAV file using a text-to-speech API. The PortalGuard server then uses SIP to connect to the customer’s SIP gateway using an extension from a pool of extensions designated for exclusive use by PortalGuard. SIP is used to dial the end-user’s phone number and play the WAV file once they answer the call. The user then types the OTP from the voice message into the PortalGuard browser interface to continue the authentication.

---

**Session Initiation Protocol (SIP)**

Voice OTPs delivered over Internet Protocol (IP)

1. User logs in through the PortalGuard web portal using their credentials.
2. PortalGuard sends a voice OTP to the user’s designated phone system.
3. The phone system sends the OTP to an out-of-band device.
4. The user inputs the OTP into the PortalGuard login interface.

---

Logon to web portal managed and protected by PortalGuard

- Random OTP generated
- OTP substituted into text-based message template
- Resulting text converted to WAV file on PortalGuard server
- SIP connection initiated from FG server to Phone System with WAV file as payload

Configure
Credential
Stores

- MS AD
- MS SQL
- LDAP

Phone System

user inputs
OTP into
required
login field

browser

Send OTP to
out-of-band
device
Appendix C: Hardware Token OTP Delivery Method

Although hardware or proprietary tokens have started to fall out of favor due to high cost and maintenance, they have still proven themselves as a viable option holding the largest market share and installed base in the two-factor authentication market. PortalGuard provides a hardware delivery method by supporting YubiKey integration.

YubiKey
This small USB-key is inserted into the user’s machine. By touching the hardware button YubiKey creates and sends a time-variant OTP by simulating keystrokes on the keyboard. The computer receives the code as though it was manually typed in by the user and PortalGuard verifies the authentication request. YubiKey avoids many issues and costs associated with other hardware tokens because the user does not have to type in the OTP, batteries are not required, and it does not rely on an absolute time generated by an accurate time source which avoids the need for synchronization.
Appendix D: Transparent Tokenless Toolbar for TOTP Delivery Method

PortalGuard’s Transparent Tokenless Toolbar (TTT) offers a way to perform multi-factor authentication by both validating the user -AND- the device they’re using. It is transparent because it has no user interface and does not impose additional processes or steps on end-users. It is tokenless because it can offer multi-factor authentication without requiring the user to possess a separate hardware-based OTP generating token/device. The workstation itself acts as the “token” or rather “something the user has” when unlocked by the user’s successful login to it. Lastly, it is implemented as a toolbar within the users’ web browsers.

After installation and a one-time, automated enrollment, the TTT automatically generates a Time-based One-time Password (TOTP) on a configurable interval and sets the value as a session-based cookie. This cookie is created for only specific websites and is encrypted using public-key cryptography to ensure only the PortalGuard server can decrypt it. The one-time enrollment data is created independently for each user and is securely stored in the user’s workstation profile. This ensures the data follows the user as they log into different workstations and allows multiple users to share the same workstation provided they have separate login accounts.

The user’s PortalGuard security policy determines what level of authentication is required. If a valid TOTP is sufficient, then the TTT can be used to effectively enable web-based SSO. For multi-factor authentication, the user is prompted for their username/password and the TOTP is used as the second factor since only workstations they have logged into will be able to generate it. The TTT is available for both 32 and 64-bit versions of Windows XP and later. It is packaged as a standard MSI so it can be silently deployed to workstations in your environment or a web page link is presented to the user upon them logging in that installs the toolbar.

Using PortalGuard’s TTT defeats man-in-the-middle attacks, which intercept messages in a public key exchange and resends them, substituting their public key for the requested key, leaving both parties with the appearance that they are still communicating with each other. PortalGuard defeats this by using an encrypted cookie designated for the valid website. The cookie is encrypted using PKI. Phishing attacks are also successfully defeated by the TTT.

- See Visio on Next Page -
Token-less Support
2FA via Transparent Token

Logon to web portal managed and protected by PortalGuard

1. Username/Password for Web Application Login

2. Browser Add-in: A transparent encrypted token (OTP) which is in time-sync with the PortalGuard server and passed from the client machine during authentication.

3. User is authenticated and granted access
Appendix E: Printed OTP Delivery Method

For cases where the user is unable to receive an OTP via traditional SMS or phone call, they have the option of generating and printing a batch of OTPs they can put someplace safe like their wallet. When the user is prompted for an OTP but hasn’t received it, they can enter the next OTP from the printed sheet. These values are still OTPs in that they can only be used for a single authentication. The user simply enters the next OTP and crosses each one out as it’s used. The printed OTPs do not expire on a set interval like standard OTPs but the user can choose to clear them or generate and print a new batch at any time from their PortalGuard Account Management page.

Printed One Time Password Support

Logon to web portal managed and protected by PortalGuard