Understanding PortalGuard’s Contextual Authentication: A Multi-factor Approach

Highlighting the Multi-factor Authentication Layer of the PortalGuard Platform
Welcome and thank you for your interest in PortalGuard's Contextual Authentication, part of the multi-factor authentication layer of the PortalGuard platform.

By the end of this tutorial you will be able to:

- Define PortalGuard
- Understand the barriers to increasing security
- Discover PortalGuard's Contextual Authentication (CBA)
- See the Step-by-step Authentication Process
- Know the Technical Requirements

Contextual Authentication: A Multi-factor Approach

Highlighting the Multi-factor Authentication Layer of the PortalGuard Platform

Notes:

Welcome and thank you for your interest in PortalGuard's Contextual Authentication, part of the multi-factor authentication layer of the PortalGuard platform.

By the end of this tutorial you will be able to define PortalGuard, understand the barriers to increasing security, discover PortalGuard's contextual authentication including see the step-by-step authentication process, and know the technical requirements associated with using PortalGuard.
What is PortalGuard?

The PortalGuard software is a Contextual Authentication platform which is focused on enhancing usability, while maintaining a balance between security, auditing and compliance for your web, desktop and mobile applications.

**Usability**
- Single Sign-on
- Password Management
- Password Synchronization
- Self-service Password Reset

**Security**
- Knowledge-based
- Two-factor Authentication
- Contextual Authentication
- Real-time Reports/Alerts

Notes:
So what is PortalGuard?
The PortalGuard software is a Contextual Authentication platform which is focused on enhancing usability, while maintaining a balance between security, auditing and compliance for your web, desktop and mobile applications.

Developed and supported by authentication experts, PortalGuard is easy to deploy, enterprise ready and tailored for an exact fit to your requirements.

To provide you with flexible options, PortalGuard offers multiple authentication methods which offer increased usability, such as single sign-on and password synchronization, and increased security with multi-factor options, such as two-factor or contextual authentication.

Slide 4

Highlights

Before going into the details...
- Configurable by user, group or application
- Stop making assumptions about who is accessing your applications
- Adjust the authentication method dynamically with every access request
- Gain insight into user access scenarios
- Cost effective and competitively priced
- Tailored Authentication for an exact fit

Notes:
Before going into the details I wanted to highlight some of the unique offerings of PortalGuard's contextual authentication. This way if you already understand the concept of contextual authentication, you can understand exactly what it is that makes PortalGuard different.

I'd like to first call out the flexibility that PortalGuard offers because you are able to configure the authentication methods for each user, group or application. With contextual authentication, you are able to stop making the assumption that a password truly represents an authorized user. By adding the user's context around the password, you can further validate the identity of each user. The user's authentication is then adjusted dynamically by PortalGuard.

Otherwise, if you weren't looking to adjust the
authentication just yet, you can gain insight into your user access scenarios by simply collecting the contextual data. Overall PortalGuard is cost effective and can be tailored for an exact fit to your requirements.

**Notes:**
Increases in roaming user populations and remote access to organizations’ confidential data is becoming a larger security concern, leaving organizations with choices to make about how to secure these resources. A conflict of interest between business groups and IT security can create a struggle to maintain usability while increasing security.

A preliminary option for organizations is to implement stronger password policies, but this poses a strong security concern, as well. When leveraging just a password to prove a user is authorized, allowing that user to have access to sensitive data is purely based on an assumption. The assumption that a password represents an authorized user, when truly it is just a password.

This has caused organizations to often over steer towards rigid two-factor authentication solutions.
Although these solutions are desirable for security, the barriers to entry for many organizations are overwhelming.

By applying stringent two-factor authentication to all users, it is not possible for the organization to adapt to all the different user access scenarios, usually resulting in poor user adoption and increased frustrations.

Due to the size and structure of these solutions, integration usually requires dedicated IT resources and training, along with the potential of additional hardware.

However, the biggest barrier is high total cost of ownership. The organization has the intention of increasing security but cannot handle the costs associated with the initial purchase and maintenance of a two-factor solution, ranging from hardware replacements to increased Help Desk calls.

So you have to make a tough decision, do you institute better password policies? Or should you implement two-factor authentication across the whole company?

Which makes you wonder…is there a midpoint between the two?
Notes:
The midpoint is referred to as "contextual authentication" which is focused on providing dynamic security to enhance usability for users and strengthen security to match your organization's policies and compliance standards.
Contextual authentication works behind-the-scenes to prevent unauthorized access and applies the appropriate level of authentication based on the expected impact of the context around a user's access request, including location, time, device, network and application.

For example, users' within your company's four walls may only need to provide strong passwords whereas a traveling salesperson or roaming user must provide two-factors. 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.

With this multi-factor approach you can now prove a user's identity beyond just knowing a simple password, by validating multiple aspects of that user's context. This removes the assumption that a password represents an authorized user and creates further barriers for unauthorized users who are trying to abuse passwords.
Notes:
As an alternative to static authentication solutions, PortalGuard understands the midpoint and handles the challenges of remote user access scenarios. By taking a cost effective, flexible approach to authentication PortalGuard offers five authentication methods: single sign-on, password-based, knowledge-based, and two-factor authentication, with the primary focus of the software platform, contextual authentication or CBA.

Using PortalGuard's CBA, organizations can now gain insight into user access scenarios. This allows them to make security and usability adjustments transparently to the user and dynamically adjust the authentication method to what is appropriate based on the user's situation.

Obtaining the user's contextual data is optional with PortalGuard's client-side browser add-on and all options can be configured down to the individual user, group or application levels.

Additional PortalGuard functionality that you should know about includes PortalGuard's two-factor authentication options which leverage soft tokens in the form of an OTP sent via SMS, email, printer or laptop; SAML single sign-on is supported with PortalGuard being able to provide a SAML token and enable web applications; Real-time activity alerts sends alerts to the admin or user regarding malicious or "Did you know" information; and PortalGuard also provides a wide array of notifications and reports for the admin to stay informed.
Slide 9
Static vs. Contextual Authentication
Duration: 00:00:25

Notes:
As you can see here, in this comparison of static and contextual authentication, the static authentication process is very rigid. The same method will always be presented to the user. Now looking at the contextual authentication process you can see how there are decisions being made along the way as to what is appropriate for the user based on their contextual access profile. This means the process is dynamic as well as flexible.

Slide 10
Benefits
Duration: 00:00:40

Notes:
PortalGuard’s flexibility, unique features and options around contextual authentication gives you tangible benefits which include:
- Increased security – without impacting the user experience
- Increased usability for authorized users while creating barriers for unauthorized users
- Flexibility - configurable to the user, group or application levels
- Lower total cost of ownership than hard token two-factor authentication alternatives
- Reduce threats using a proactive approach
- Gather Insight – analyze contextual data reports

- Increased security without impacting the user experience
- Increased usability for authorized users while creating barriers for unauthorized users
- Flexibility by being able to configure PortalGuard to the user, group or application levels
- Lower total cost of ownership than hard token two-factor authentication alternatives
- You can take a proactive approach to reducing threats by blocking suspicious users in real-time before a login attempt is made
- And gather insight about your user community by analyzing the contextual data reports PortalGuard provides
Before getting into how PortalGuard’s contextual authentication works, it’s important to understand the following terminology:

An Authentication method is the type of authentication the user will be presented with. PortalGuard includes the following methods.

- Single sign-on: username and password (single password for multiple systems)
- Password-based: username and password
- Knowledge-based: username, password and challenge question
- One-time Password (OTP): username and OTP
- Multi-factor: username, password and OTP or contextual data

A credibility score is the numeric value that is used to determine the appropriate authentication method based on a set of ranges. The credibility score is determined from the credibility policies. Here is a helpful chart which shows that the higher the score the more credible a user is, but with a lower number the user is considered risky.

A credibility policy is a configurable policy based on categories and identifiers to which you can assign a score. A credibility policy can have multiple categories. Let’s dig into the credibility policy definition a little further.

A category is a collection of related identifiers or context, which currently includes device, time, location, and network. A category can have multiple identifiers.

An identifier is an individual attribute that is assigned a score based on their importance. For example the category is time, and the identifiers would be office hours, after hours, and weekend hours.

The last piece of the credibility policy is the weight, which is an optional percentage for each category that adjusts the category’s impact on
Finally, the application realms identify an application and assigns a weight to that application that adjusts the overall credibility score. So say the application realm is 50% and the user’s score is 100, after the realm is enforced the user will have a score of 50.

When implementing CBA it is recommended to run analysis mode first, to establish a baseline for the environment. This would run the CBA process in its entirety but stops short of adjusting the authentication method for the user. This allows you to establish a suitable configuration, collect reports, and determine the possible effects on your user community. After a recommended period, typically 60-90 days, the adjustment of the authentication method can be enforced to directly affect your user community.

To turn on CBA, an administrator simply checks a box on the desired security policies which contain either individuals or groups of users. In order to collect the contextual data around a user’s access request PortalGuard uses an
installed browser add-on. This is installed using a standard MSI and can be pushed out silently. Although the add-on is optional, users without the client-side software installed are considered “unmanaged” and can be given a lower credibility score due to the lack of actionable context data.

Now for the step-by-step process which is completed every time an access request is received. PortalGuard also supports CBA for password resets, recoveries, and account unlocks.

The user begins the login process by entering their username and clicking “Continue”.

The next three steps happen behind the scenes, transparently to the user and within milliseconds. The contextual data is sent from the client-side browser add-on to the PortalGuard server. The PortalGuard server identified the user’s credibility policy and computes the following:
- The user’s gross score for each category
- Any category weight which has impact on the score
- The net score from the policy and calculated weights
- And any modifications due to the sensitivity of the requested application

The PortalGuard server looks up the appropriate authentication method using the final credibility score and previously set ranges which the administrator configured. PortalGuard enforced the appropriate authentication method for the user’s current access attempt, such as two-factor authentication as the dialog shows. The user now completes the login process and access is granted.
All the following settings are policy specific, so you can have different values for different users/groups/hierarchies.

Features that are Configurable through the PortalGuard Configuration Utility include:

- Enabling or disabling contextual authentication
- Assigning users or groups to individual credibility policies
- Within the credibility policies you can configure
  - The client type
  - Enforce category weighting
  - Enforce application realms
  - Display a helpful scoring UI
  - Define categories, weights, and identifiers
  - Determine the credibility score for the policy
- For the credibility score you can configure default ranges including
  - Their start and end scores
  - The authentication type which will be enforced
  - And whether alerts should be turned on or off
- The last piece to configure is the application realms which allows you to specify the application name, modifier percentage, and servers.
Notes:
Implementation of the PortalGuard platform is seamless and requires no changes to Active Directory/LDAP schema. A server-side software installation is required on at least one IIS server on the network. Additional client-side software is required with contextual authentication in the form of the browser add-on which is installed using a standard MSI and can be pushed out silently.

Notes:
A MSI is used to install PortalGuard on IIS 6 or 7.x. The MSI is a wizard-based install which will quickly guide you through the installation. This version of PortalGuard supports direct access and authentication to cloud/browser-based applications, only. PortalGuard can be installed directly on the following web servers, most commonly on IIS. The PortalGuard Web server also has the following requirements on Windows operating systems. PortalGuard is fully supported for installation on virtual machines and can currently be installed on the following platforms.

- **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**
- **.NET 2.0 framework or later must be installed**
- **(x64 only) Microsoft Visual C++ 2005 SP1 Redistributable Package (x64)***
- **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**
Thank you for taking the time to learn more about PortalGuard's Contextual Authentication. Please click the Attachments button at the top of this tutorial for a copy of this content in PDF format. For more information please visit PortalGuard.com.