

A BIO-key® Solution.

Tech Brief

Contextual Authentication: *A Multi-Factor Approach*

Table of Contents

<u>Summary</u>	3
<u>The Basics</u>	4
<u>PortalGuard Contextual Authentication (CBA)</u>	5
Contextual Authentication vs. Static Authentication	5
<u>Features</u>	6
<u>Benefits</u>	6
<u>CBA Terminology</u>	7
<u>How It Works</u>	9
Analysis Mode	9
Client-side Browser Add-on	9
CBA Process	9
<u>Configuration</u>	11
<u>Deployment</u>	12
<u>IIS Install</u>	12
<u>System Requirements</u>	13
<u>Schedule a Demo</u>	14
<u>Platform Layers</u>	14

Summary

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. Although instituting better password policies is a preliminary option, organizations are often over steering 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?

The Basics

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.

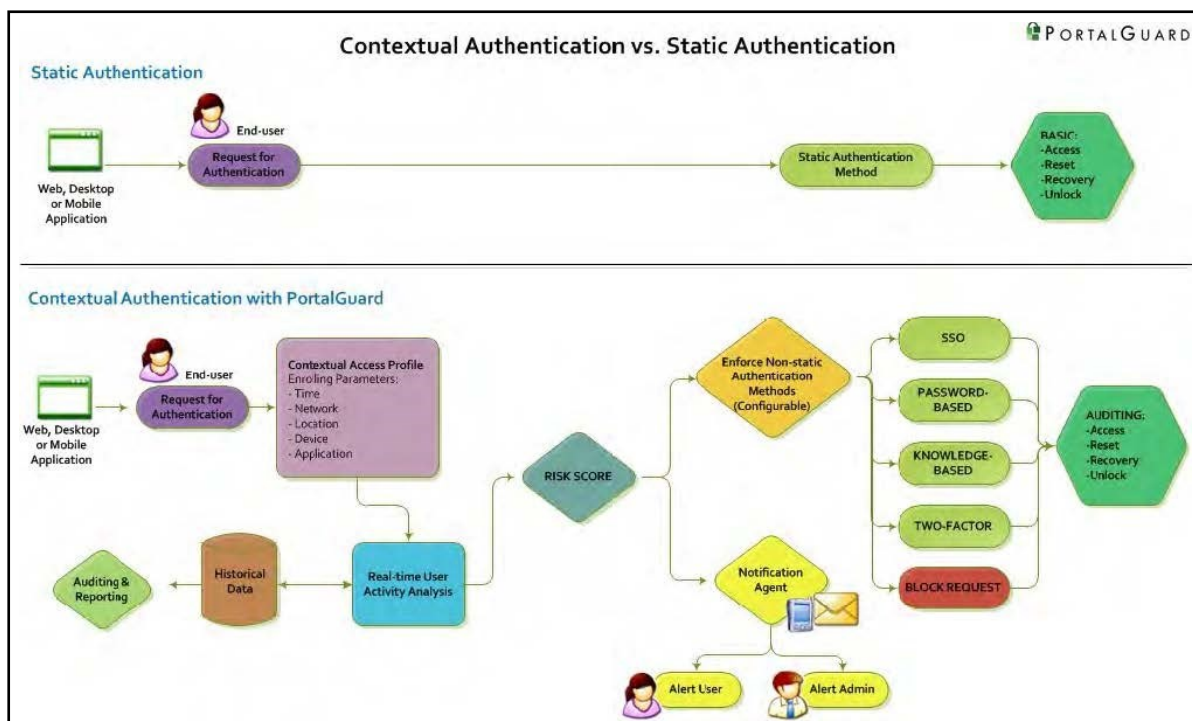
For example, users’ within your company’s four walls may only need to provide strong passwords whereas a traveling salesperson or roaming user must provide Two-Factors. However, a traveling salesperson now in the office only needs to provide a password to prove his identity due to his new situation when requesting access.

PortalGuard Contextual Authentication (CBA)

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 methods of authentication (Single Sign-On, Password-Based, Knowledge-Based, Two-Factor Authentication, and block a request) with the primary focus of the software platform being CBA.

Using PortalGuard's CBA, organizations can now gain insight into user access scenarios allowing 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 and all options can be configured down to the individual user, group or application levels.



Features

- Provides five different authentication methods – Single Sign-On, Password-Based, Knowledge-Based, Two-Factor, and blocking a request
- Contextual Authentication (CBA) –applies the appropriate authentication method for each access request depending on the user's context
- Client-side browser add-on – optionally obtain users contextual data such as location, time, network, and type of device used
- Provides Two-Factor Authentication by delivering a One-Time Password (OTP) to a user via SMS, email, printer, or to their laptop in the form of a transparent token (i.e. the client-side browser add-on producing a cookie)
- SAML Single Sign-On: can create a SAML token and enable SAML Single Sign-On to Cloud/Web-based applications to accept SAML tokens
- Real-time Activity Alerts – alerting the admin or user to malicious activity or "did you know" information
- Notifications – including emails to a user of access with their account from a new device
- Reporting Tool – contextual data reports allow you to take real-time action on meaningful situations
- All events are stored in a SQL database for easy auditing and reporting

Benefits

- Increase Security without impacting the end-user experience
- Increase Usability for authorized users while creating barriers for unauthorized users
- Configurable – to the user, group or application levels
- Lower Total Cost of ownership than token-based Two-Factor Authentication alternatives
- Proactive approach to reducing threats - block suspicious users in real-time before a login attempt is made
- Gather Insight – analyze the contextual data reports PortalGuard provides

CBA Terminology

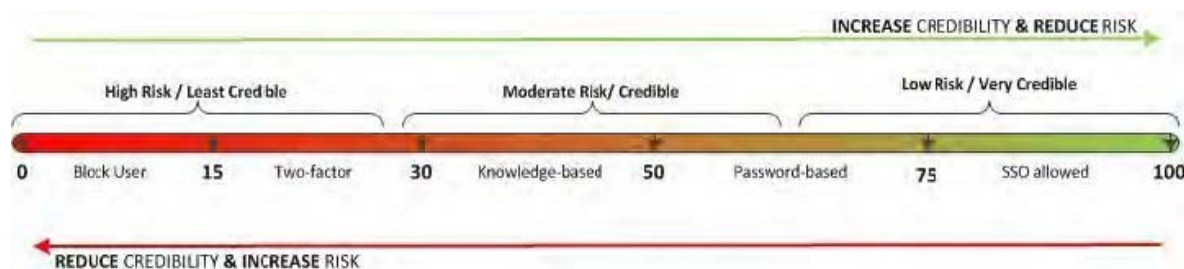
Authentication Methods:

The type of authentication the user will be presented with:

- 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
- Two-Factor: username, password and OTP

Credibility Score:

The numeric value that is used to determine the appropriate authentication method based on a set of ranges - determined from credibility policies.



Credibility Policy:

Configurable policies based on categories and identifiers to which you assign a score. A credibility policy can have multiple categories.

- **Category** - collection of related identifiers (context); currently includes device, time, location, and network. A category can have multiple identifiers.
- **Identifier** - individual attributes that are assigned scores based on their importance (Ex. Time: off hours, office hours, and weekend hours)
- **Weight (%)** - an optional percentage for each category that adjusts the category's impact on the credibility score versus other categories

Application Realms

Identifies an application and assigns a weight (%) to that application that adjusts the overall credibility score (Ex. The application realm is 50% and the current score is 100, after the realm is enforced, the user has a score of 50).

Credibility Policy



Use this dialog to create a new or edit an existing credibility policy. Categories are used to group the chosen identifiers. Make any changes and click 'Save' to commit them. Clicking 'Cancel' will not save any changes.

Name: Development

Description: CP for development

Client Type: Managed

Enforce Auth Decisions: ☒ Enabled

Use Category Weighting: ☐ Enabled

Enforce Application Realms: ☐ Enabled

Display Scoring In UI (Debug): ☒ Enabled

Maximum possible score: 240.00

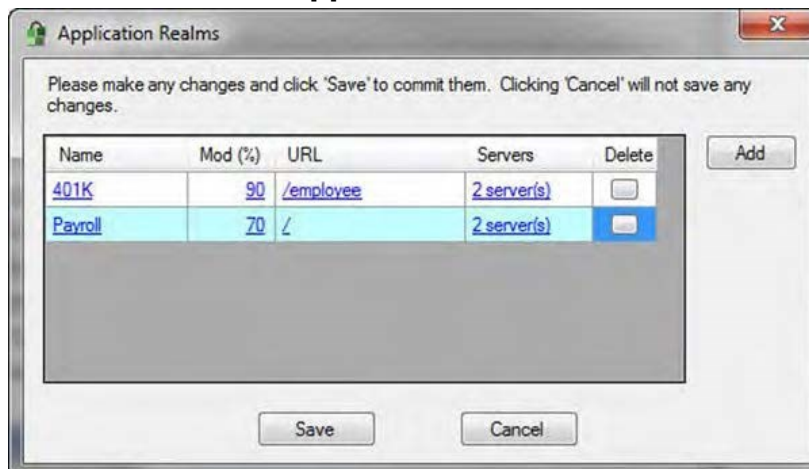
Categories

Type	Identifiers	Delete
NETWORK	LAN(60), Wireless auth WEP(20), D...	<input type="checkbox"/>
LOCATION	Main office(80)	<input type="checkbox"/>
TIME	Work hours(30)	<input checked="" type="checkbox"/>

Add

Save Cancel

Application Realms



Please make any changes and click 'Save' to commit them. Clicking 'Cancel' will not save any changes.

Name	Mod (%)	URL	Servers	Delete
401K	90	/employee	2 server(s)	<input type="checkbox"/>
Payroll	70	/	2 server(s)	<input checked="" type="checkbox"/>

Add

Save Cancel

How It Works

Analysis Mode

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.

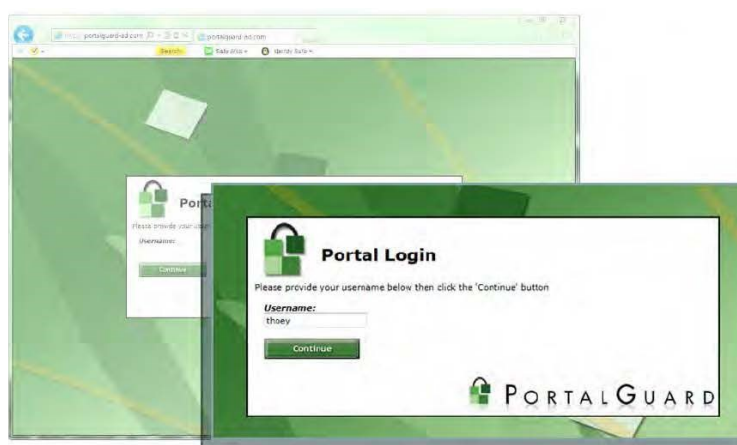
Client-side Browser Add-on

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.

CBA Process

The following process is completed every time an access request is received. PortalGuard also supports CBA for password resets, recoveries, and account unlocks.

Step 1: The user begins the login process by entering their username and clicking "Continue".



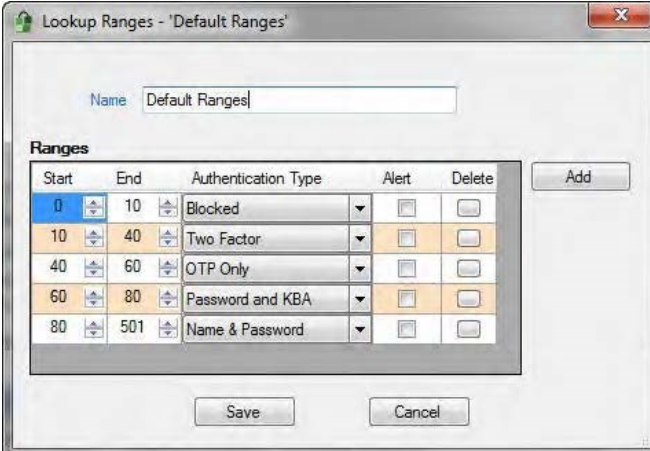
NOTE: Steps 2-4 happen behind the scenes, transparently to the user and within milliseconds.

Step 2: Contextual data is sent from the client-side browser add-on to the PortalGuard server

Step 3: The PortalGuard server identifies a user's credibility policy and computes the following:

- Gross score for each category
- Any category weight impact to the score
- Net score from the policy and weights
- Modification due to sensitivity of requested application


Step 4: The PortalGuard server looks up the appropriate authentication method using the final credibility score and previously set ranges which the administrator configured.



Start	End	Authentication Type	Alert	Delete
0	10	Blocked	<input type="checkbox"/>	<input type="checkbox"/>
10	40	Two Factor	<input type="checkbox"/>	<input type="checkbox"/>
40	60	OTP Only	<input type="checkbox"/>	<input type="checkbox"/>
60	80	Password and KBA	<input type="checkbox"/>	<input type="checkbox"/>
80	501	Name & Password	<input type="checkbox"/>	<input type="checkbox"/>

Step 5: PortalGuard enforced the appropriate authentication method for the user's current access attempt. The user provides the required credentials to successfully complete their access request and login.

Ex. Two-Factor Authentication



One-Time Password Required
 A One-Time Password (OTP) has been sent to your phone. It could take 10-15 seconds to be delivered.
 Upon receipt, please enter the OTP below to login.

Username:

Password: Show password ☐

One-Time Password:

Log On Cancel

Configuration

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

Configurable through the PortalGuard Configuration Utility

- Enable or Disable CBA
- Assign users or groups to individual credibility policies
- Credibility Policies
 - Client Type
 - Use Category Weighting
 - Enforce Application Realms
 - Display Scoring UI
 - Categories
 - Weight
 - Identifiers
 - Credibility Score
- Default Ranges
 - Start and End Scores
 - Authentication Type
 - Alert On or Off
- Application Realms
 - Application Name and URL
 - Modifier %
 - Servers

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 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.

IIS Install

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

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:

- 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

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

PortalGuard works with Windows Terminal Services on Win2003 servers and Remote Desktop Services on Win2008 servers.

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.

Schedule a Demo

Interested in seeing a demo of PortalGuard's CBA offerings?

[Schedule a Demo](#) today!

Platform Layers

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

- Tokenless Two-Factor Authentication
- Self-Service Password Reset
- Real-time Reports / Alerts
- Knowledge-Based
- Password Management
- Single Sign-On

