A BIO-key® Solution.

White Paper

The Fastest and Safest Way to Secure Access to SharePoint

Copyright © 2020 BIO-key International. All Rights Reserved.

Table of Contents

Copyright © 2020 BIO-key International. All Rights Reserved.

When External Users Must Identify Themselves

The Use Case

The business case for external authentication and identity management is clear. To set the stage, let us consider an all too typical situation for extending an existing SharePoint site to include external users.

Suppose, as the national distributor for precision mechanical devices, your company has invested substantial time and money toward developing a technical resources portal. This portal, powered by SharePoint, exists primarily to support your internal sales reps and customer service engineers. Once authenticated on the corporate intranet, employees easily access the portal and find detailed information about various devices, as well as interactive maintenance guides and configuration applications.

Fortunately, business is good and the market is growing rapidly. Your firm's executive team plans to capture this growth by adding new distribution channels, and relying on partners and enterprise customers to develop specialized business solutions. As part of the channel strategy, your executives promise to make it easy for the sales and support specialists in these third-party firms to access the technical resources portal powered by SharePoint.

As the portal maintainer, you are now responsible for providing an ever-growing number of external users with simple and secure access to your SharePoint site.

The Authentication Dilemma

Herein lies the dilemma for empowering these new channels: simply making the content publicly available over the Web is not an option. The technical resources portal houses proprietary information and applications, all of which need to be secured against malicious attackers. In order to maintain this security, access to your SharePoint portal needs to be strictly controlled.

To add an additional hurdle, sales and support specialists in third-party firms are not registered on your corporate intranet. In order to support these individuals, you need to extend the capabilities of your portal and support an external SharePoint site. Further extending the security and access scenarios for SharePoint brings with it another obstacle: a dramatic increase in Help Desk calls, all of which need to be addressed professionally and successfully in a timely manner.

Expectations are clear. Partners and customers expect seamless access where they can easily establish their online identities and recover their credentials when they need to. As far as these users are concerned, good authentication is like good plumbing: things just work and are rarely noticed.

From your perspective as the portal maintainer, you want to authenticate these external users with minimal administrative overhead, while continuing to ensure the security of the information and applications housed within SharePoint. In fact, you may want to mitigate the risks of unauthorized access from outside your intranet by enhancing authentication using a fully integrated package designed with SharePoint in mind.

Moving Beyond Manual Process

The reality is very different. A SharePoint site running on a corporate intranet relies on a local user repository (Such as Active Directory, LDAP, or SQL) to authenticate employees. By default, these repositories support none of the necessary capabilities for managing the identities of external users. Without additional features and functionality, site administrators are responsible for a host of additional tasks, such as:

- Manual user registration
- Initial password creation
- Password reset/recovery
- Updating Account Details
- Etc.

These manual processes add time and cost to operations. In addition, these processes are not scalable and do not fully address the security risks of authenticating external users.

Moreover, manual processes are not a satisfactory solution for any growing or expanding organization. Rather, they are a barrier to the success of your executives' plans and your firm's growth strategy. A fully integrated authentication package provides unobtrusive authentication for seamless security, coupled with a range of self-service solutions for identity management.

Benefits of an Integrated Authentication Package

Utilizing a fully integrated authentication package alongside SharePoint allows organizations of any size to properly manage both internal and external users without requiring additional resources.

White Labelling - Inspire Confidence and Reliability

White label design is a staple for any worthwhile solution, especially one that provides access to local and remote users alike. Unfortunately, the stock SharePoint login portal is not customizable, and is not well suited for constant access from both ends of the spectrum.

A fully integrated authentication package allows organizations to streamline the login by providing a fully customizable page to match the look and feel of the surrounding website. When users reach a login page, they need to be reassured that they are in the right location. Implementing a custom login page inspires confidence and assures end users that it is safe to proceed. Furthermore, adopting Bootstrap or a similar framework as a standard ensures your SharePoint site is accessible from any device, whenever necessary.

Integrated as part of a complete package, white label design provides organizations with additional benefits as well, such as:

- Improved User Experience
- Rapid User Adoption
- Enhanced Reliability

A Complete Package of Features and Services

While White Label Design is a must have feature, it is part of a much larger group of features and services which vastly improve the inherent functionality of SharePoint. In addition, a fully integrated authentication package is a one-stop-shop for increased SharePoint functionality for external user support.

Copyright © 2020 BIO-key International. All Rights Reserved.

A Full Suite of Self-Service Capabilities

Self-Service Registration

With external users needing access to your SharePoint portal, registration is an important factor. Out of the box, SharePoint requires administrators to manually process access requests to create accounts in the local user repository. It is not neat, and it is not fun.

A fully integrated authentication package provides organizations with Self-Service capabilities to reduce the necessary administrative oversight. New users simply fill out the required, predefined information, and are automatically registered and stored in the appropriate user database. Existing user data is imported automatically, improving migration and further improving the user experience for existing users**.**

The entire process is bound by existing policies and requirements, and works to provide external users with rapid access, without bogging down your local IT resources.

Self-Service Password Management

- Password Reset for forgotten or expired passwords
- Password Recovery where a complete reset is unnecessary
- Account Unlock for inaccessible accounts.

The continued lack of password management features in SharePoint further complicates the relationship between users and existing SharePoint sites. Often, adding extranet functionality vastly increases the workload of the local IT Help Desk due to a significant increase in forgotten passwords or locked accounts.

A full suite of Self-Service functionality removes this additional drain on local resources, and provides end-users with the ability to continue working without interruption. Administrators need not sacrifice security either, as multiple methods become available for verifying user identity prior to a successful self service action. Methods include:

- Multiple OTP delivery options
- Mobile Authentication
- E-mail verification
- Challenge Questions & Answers

Self-Service requirements are even customizable at the user repository level, ensuring that each user is provided with the correct capabilities to ensure optimal usage of their newly accessible site.

Accessible from Any Device

Utilizing Bootstrap for a completely responsive design, SharePoint integration goes beyond the standard desktop experience. Portal access and self-service functionality can be initiated on any device:

- **Cell Phone**
- **Tablet**
- **Laptop**
- **Desktop**

Support for multiple devices ensures that your end-users always have a a consistent and optimal viewing experience - complete with easy reading and navigation - regardless of the device being used.

Multi-Factor Authentication

Exposing SharePoint to the extranet brings with it a host of security considerations. Chief among these concerns is the ability to securely validate remote users. Providing support for multi-factor authentication enables any organization to verify a user's identity through various channels:

- Challenge Questions & Answers
- One-Time Password flexibility
  - E-mail
  - SMS Text Message
  - Mobile Authenticator
- Hard Tokens
- Risk-Based Authentication

Whatever your security policies require, an integrated authentication solution provides enough flexibility and usability to improve security without sacrificing usability.

Single Sign-On (Reduce attack surface)

Many SharePoint implementations contain links or access avenues to additional applications or services. Each of these will also require authentication for various users, and continual login prompts can be a sincere burden on users and administrators alike.

Single Sign-On (SSO) provides organizations with a secure method of allowing users to access these applications and services without inconveniencing them or interrupting their process to remember additional credentials. Many applications retain authentication requirements of varying complexity. SSO uses a standards based approach to provide the flexibility needed to integrate many applications into a single, initial login.

In addition, SSO enhances attack surface reduction by reducing multiple potential access points to a single, secure login. With a fully customizable login portal leading to SharePoint, users can leverage those credentials to safely access any necessary applications.

Single Log-Out

Single Log-Out (SLO) is a separate but related feature to SSO. When SSO sessions are completed, many users are likely to simply close the browser and hope for the best. SLO ensures that each session is terminated properly, preventing any unauthorized access to an idle or potentially vulnerable account.

With external access as a priority, unobtrusive security features deeply ingrained within a solution are an absolute must. Users want usability and administrators want security: a strong integrated authentication package provides both without the hassle.

Multiple Directory Support

There is no guarantee that your organization is going to rely entirely on Active Directory. In fact, many organizations implement multiple directories within a given environment: Active Directory, LDAP, and even various SQL instances. The use case for this scenario is various and contingent upon the requirements of an organization. An integrated authentication package provides the flexibility to support multiple directories both individually and simultaneously.

Suppose that exposing SharePoint to the extranet requires your organization to implement additional user repositories to assist with segmenting your incoming user base. Your internal users will remain on the local directory, while newly registered external users will be put into a remote user database using SQL.

Instead of searching for additional solutions, an integrated authentication package seamlessly filters users accordingly without impacting the end-user experience or undercutting the necessary security policy requirements. In the case of extranet SharePoint access, such a use case reduces risk and maintains a high level of security and access management.

Exposing SharePoint as an extranet site is not a task to take on lightly. Between improving usability and maintaining security, the necessary requirements of such a project are never as simple as flicking a switch. With a fully integrated authentication package however, the deployment becomes much more manageable and even serves to enforce security from top to bottom.

Enforcing Best Practices

An important consideration when implementing any authentication solution is to understand the best practices and enforce them accordingly. With multiple solutions existing simultaneously, tracking and upholding various best practices is an administrative nightmare.

A fully integrated authentication solution for SharePoint works to reduce that load by streamlining authentication best practices and helping administrators enforce them with significantly less effort.

More Best Practices to Consider

Password Policies

Password policies are important security measures that can make or break the security of your login portal. When opening SharePoint up to external users, enforcing password policies is an import method of securing the front door against malicious attackers.

An integrated authentication package supports password policies down to the individual organizational unit used to define a user in a given repository. Administrators simply need to set the policy and walk away – the solution enforces it while providing users with the capabilities required to remain securely within the appropriate bounds of their policy.

Increased Security for Remote Access

When extending SharePoint to external users, it is important to provide the highest level of security possible, without becoming detrimental to the end-user experience. An integrated authentication package provides many tools to achieve this goal and provide users with a simple, beneficial experience while accessing your extranet SharePoint site.

- Stronger Authentication Requirements (CBA, OTP, etc.)

As an additional best practice, stronger authentication requirements can be configured for users based on various factors such as which information an account can view, or whether or not they are an external user. Depending on the situation, an integrated authentication solution allows for stronger or less stringent security measures to be required of users based on each account, their group, or other organizational unit.

- Contextual Authentication

Contextual Authentication is a form of Risk-Based Authentication that adjusts security requirements based on the specific access scenario of a login attempt. Various elements are taken into consideration for contextual authentication, such as:

- Time
- Location
- Network Type
- Wi-Fi Security
- And more!

With Contextual Authentication, a risk score is attributed to various aspects of an access scenario, and the authentication process is adjusted accordingly. For more information, check out our in-depth Tech Brief on Contextual Authentication.

A fully integrated authentication package provides you with the tools to increase security at every level during your SharePoint extranet deployment.

The Business Value of PortalGuard for SharePoint

An integrated authentication package fills the gap where other solutions leave organizations wanting. Often, when specific features or functionality is not available, organizations resort to home grown or open source solutions that remain largely unproven for both security and usability. Today, PortalGuard is well positioned to be your standard for an integrated authentication package.

In addition to the primary features and services provided, the combined value and advantages of PortalGuard as a fully integrated authentication package encapsulates over 120 different features. With such wide reaching flexibility, PortalGuard fits well in any environment, and has been constructed and designed with SharePoint in mind.

For proper deployment of SharePoint to external users, you need a solution that is poised to stand the test of time. As a fully managed solution, PortalGuard is an evolving security tool that proactively fights against cyber hacking both on-premises and in the cloud.

Copyright © 2020 BIO-key International. All Rights Reserved.

About Us

About PistolStar, Inc.

PistolStar, Inc. is an authority in consolidating multiple web apps while providing a secure, trustworthy experience for end-users that interact with login portals on a daily basis. Whether the need is to remain compliant, to address specific end-user concerns, or simply to find a solution that fits perfectly in a given environment, PistolStar approaches the concepts of trust, security, and convenience through a fully customizable, white-label portal experience.

About PortalGuard®

The flagship product, PortalGuard, supports true Single Sign-On functionality alongside Multifactor Authentication and granular Self-Service capabilities. The software works either as a strong, stand-alone front door or as a fully integrated addition to existing CMS or other portal installations. While small to medium sized businesses and organizations are the biggest target audience for the PortalGuard solution, the software is fully scalable to support both high and low end-user volumes without any deterioration of service or functionality.

Put simply: PistolStar competently delivers secure integration without compromising security