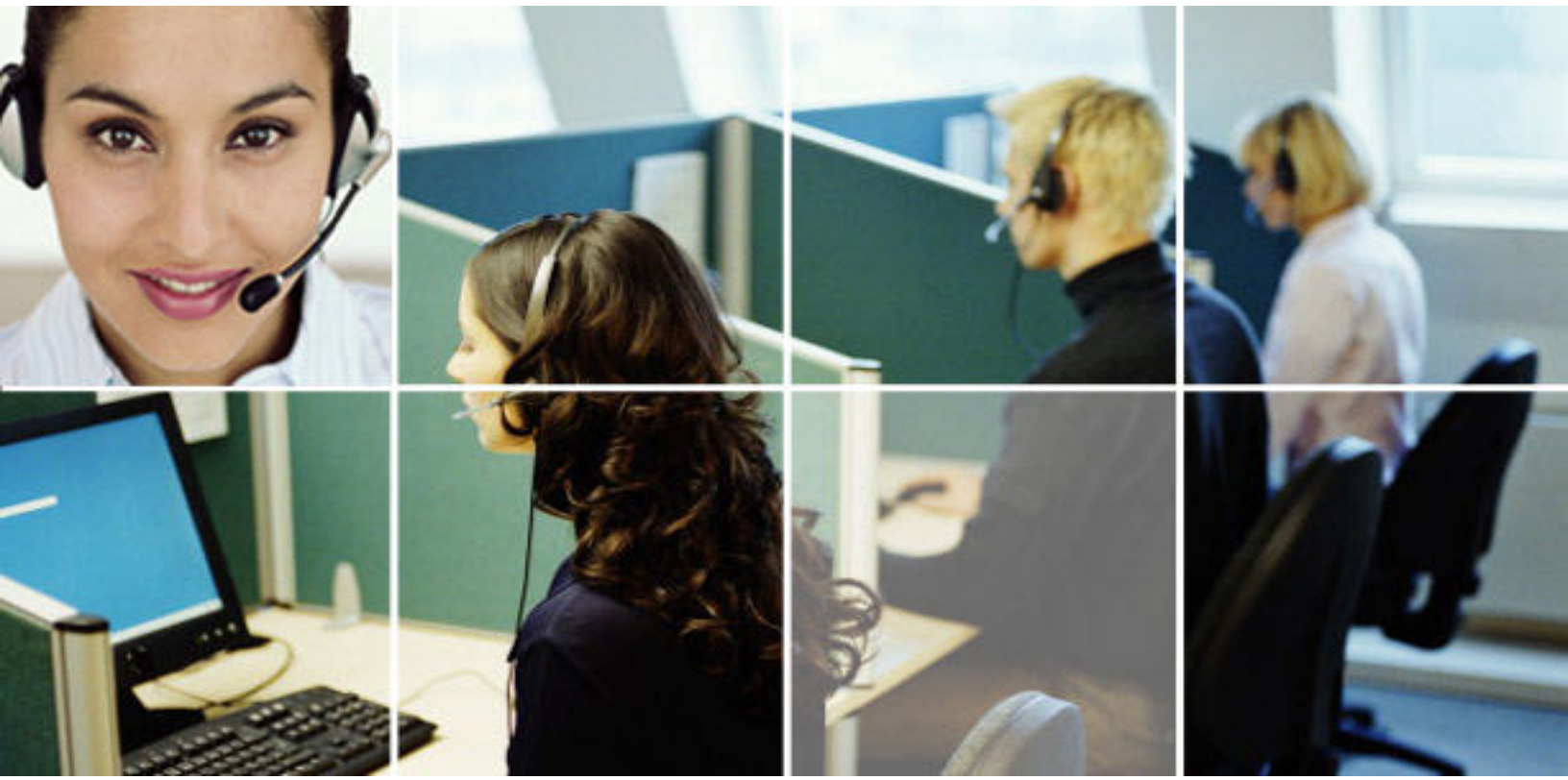
Novo Solutions, Inc.
Innovative, Customer Support Solutions

Application Authentication & Authorization

The Benefits of Integrated Authentication



A Novo Solutions Executive Business Brief

Application Authentication & Authorization

Introduction

This paper will discuss an overview of application authentication and authorization, the problem that arises as a result of multiple authentication systems and the resulting cost to an organization. Integrated authentication and authorization will be presented as the solution along with the benefits to an organization. We will conclude by introducing how the Novo Service Desk and its add-on modules provide methods for this type of integration and the benefits that arise as a result of using these methods.

Overview of Application Authentication & Authorization

- A Definition of Terms

Before we begin our discussion, it is important to define what is meant by the terms authentication and authorization. Simply stated, authentication refers to the process of identifying the user. Authorization, however, refers to what the user has access to. The importance of controlling who has access to what information should be apparent to most organizations and is outside the scope of this paper.

The Problem

Most organizations do not have a single application that fulfills all of their business needs. While it is a desirable goal to have as much integrated functionality within a single application as possible, even large, very expensive enterprise systems rarely address every need in the desired way. As a result, organizations must consider supplementary applications to address these specific needs. A problem that arises when additional applications are added to the network (intranet /extranet or both) is the issue of burdening the users with an added application to have to login to.

Administrators and End Users have enough work to do as it is and adding the obstacle of having to sign into multiple applications is less than ideal. End Users are forced to keep track of multiple passwords and the hassle of additional steps to do their work. In addition to this, network and application administrators are faced with the challenges of adding users to each system, keeping track of who has access to what and somehow keeping user names updated or synchronized between systems.

Some of the costs to an organization for these inefficiencies are:

- Decreased Productivity of high skilled Network & Application Administrators
- Reduced Benefits – In some cases users may tend to use the application less than they should because of the hassle of accessing it, forgetting their password, etc. In the case of a Help Desk or Knowledge Base system, this can result in bad behaviors (calling the Help Desk instead of submitting a ticket, not following best practices because they did not review the procedure documented in the Knowledge Base, not documenting and sharing knowledge, etc.)
- Exposure to Risk – When application access is difficult to manage, someone could gain access to information they should not have (i.e. when an employee leaves the organization, etc.)

The Solution – Integrated Authentication & Authorization

To effectively address the problems listed above, it is important that a new application being added to the network be able to tie into the existing authentication system. This is not just for the benefit of network and application administrators (i.e. maintaining a central login management system). It also provides a way for end users to be able to login to the network (or extranet web site) once and automatically have access to the applications and resources they need to effectively perform their jobs. Some applications that do provide single sign in modules often stop there – only providing benefits for authentication (definition listed above). An even higher level of benefit is achieved when the application not only provides single sign on capabilities, but also allows administrators to use a centralized system (i.e. Microsoft Active Directory) to control some level of what users have access to in the new application (authorization).

Some of the benefits to an organization of single sign-on access are:

- Increased Productivity - Simplicity of user management for administrators and reduced barriers for end users accessing the information and resources they need
- Improved Benefit/ROI – When applications are used more often for what they were designed to do, the organization receives the resulting benefit and achieves a quicker return on investment.
- Reduced Exposure to Risk – Provided when a greater degree of control of application access is maintained.

How the Novo Solutions – Novo Service Desk Handles Authentication and Authorization

For the purpose of this discussion the Novo Service Desk (integrated Knowledge Base, Help Desk, Asset Manager) will be referred to, though each individual Novo Solutions application uses the same core user management system.

Before we discuss the specifics of how to achieve integrated authentication and authorization with the Novo Service Desk it is important to understand the types of users that can be configured. The two types are:

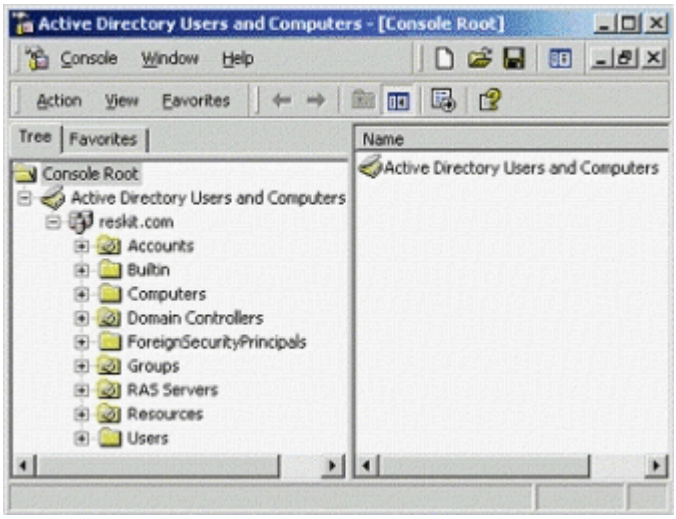
1. Admin Users – These users can be configured with to do things such as add articles to the Novo Knowledge Base, manage and respond to tickets in the Novo Help Desk, add and manage assets in the Novo Asset Manager. Admin Users can also be segmented into one or more security groups and be assigned to different roles within those groups providing a very high level of configurability.
2. End Users – These users (who can be internal employees, external customers or both) can be configured to view and search knowledge base articles, submit help desk tickets and view a list of assets assigned to them. When using the Novo Knowledge Base, End Users can also be segmented into different “portal” views. This allows Admin Users to publish certain articles to one group of users while blocking them from other groups (i.e. different employee departments or different customer types). End Users can also be associated with an Account/Company, thus allowing them to be grouped together (i.e. when there are multiple contacts at a customer site).

Methods of Authentication Available with the Novo Service Desk:

- **Built in Forms Based Authentication**
  - Typical Use: When the system is accessed directly, primarily by external customers

- What it Does: A web based login screen provides a way for both admin and end users to login to the Novo Service Desk
- Configuration Requirements: None

- **Microsoft Active Directory**
(additional module required)
  - Typical Use: When the system is primarily accessed by internal employees that login to the network via Microsoft Active Directory. This module works with both Admin Users and End Users.
  - What it Does: Provides seamless authentication & authorization. If someone is logged into the network; they will be automatically logged in to the Novo Service Desk when they access it.
  - Configuration Requirements: 1) Microsoft Active Directory must be used for network authentication, 2) Administrator access to the Web Server and to Microsoft Active Directory.



- **3rd Party Authentication** (additional module required)
  - Typical Use: When end users already login to another web based system (i.e. an intranet/extranet system). This module automates End User authentication only – it does not automate Admin User authentication.
  - What it Does: Allows a programmer to create a button/link that passes user information to the Novo Service Desk providing automated authentication. User information is automatically imported and/or refreshed.
  - Configuration Requirements: 1) Programming knowledge, 2) Knowledge of the user authentication system of the 3rd party application (to authenticate from)
- **Web Services API** (additional module required)
  - Typical Use: When "behind the scenes" automated authentication needs to take place to allow data (in the Novo Service Desk) to be added, updated or viewed through the back end (i.e. not through the web interface).
  - What it Does: Allows a programmer to develop methods to interact with the Novo Service Desk in ways that provide seamless integration
  - Configuration Requirements: 1) Programming knowledge, 2) Knowledge of application integration

Conclusion

In summary, we have seen the problems caused by adding applications to a network that do not integrate with existing authentication systems. Some of the resulting costs to an organization as a result are decreased productivity, reduced benefits from lower application use and exposure to unauthorized access to information. The solution of integrated authentication and authorization was presented along with the anticipated benefits such as increased productivity, faster ROI and minimizing risk of exposure to unauthorized access. We concluded with an overview of how the Novo Service Desk provides various methods for single sign in authentication and authorization.

Contact Novo Solutions, Inc. to learn more about how our robust, flexible and easy to use web based solutions can help you solve key problems related to providing customer or technical support, capturing and sharing knowledge and managing IT and other related assets.

Novo Solutions, Inc.
(888) 316-4559 USA
(757) 687-6590 USA
020 8002 9853 UK
sales@novosolutions.com
www.novosolutions.com