White Paper

User Creation and Authentication in Remedyforce

Getting Started with Remedyforce Series

Brian Zentner – BMC Software, Inc.

Kedar Zavar - Cloud*action*

31 March 2015

Welcome to the “Getting Started with BMC Remedyforce” Series

Today’s IT departments must drive business growth and innovation, while coping with less resources and increasing complexity. To do this, they require an IT Service Management solution that provides best practices while minimizing costs. BMC Remedyforce is built on Salesforce—the world's most widely used cloud platform—to deliver complete IT service management functionality with the secure social, mobile, and collaborative capabilities users expect.

With the “Getting Started with Remedyforce” white paper series, our aim is to help you leverage BMC Remedyforce to improve the effectiveness and efficiency of your ITSM operations. Each paper addresses a specific area of interest and provides you with conceptual, functional and technical best practices to make configuration decisions and take action to gain value from your BMC Remedyforce investment.

Remedyforce Users, Creation and Authentication

Creating users (and granting those users the ability to login into the Salesforce Platform to access the Remedyforce application based on a set of permissions, profiles, and roles) is critical to the functionality of your Remedyforce implementation and the security of the data contained in your system. The purpose of this whitepaper is to explain the types of user creation and authentication methods available, and the considerations that need to be made when determining what method of user creation and authentication best supports your organization.

Users, Profiles, Roles, and Permission Sets

User accounts contain data specific to the individual user, and settings that grant access to installed applications and data contained in those applications. In this section, we’ll explore the components of user configuration that determine the Remedyforce user experience.

Users

User accounts are required so that your staff and customers can access the Remedyforce application. These user accounts contain general information such as: username, email address, contact information, etc. They also contain information that is vital to grant and/or restrict access to application features and data through the use of roles, profiles, and permission sets. When authenticating to the Remedyforce environment, these permissions are applied and access is granted to specified data types and application field and form access. This can be done automatically through integration to your LDAP server, or can be managed manually by your Remedyforce administrator.

Profiles

When a user is created, they are granted access to applications, the fields within the applications, and the forms that contain those fields. This is accomplished through the use of ***profiles***. These profiles are created to use different Salesforce license types. Leveraging profiles to create custom application access to your users is vital in ensuring any modules within an installed application is being accessed by only those who should have access to them. Custom profiles can be created with field level granularity to ensure application security to varying groups of users who will access your Remedyforce instance.

Roles

Data security is a top priority for most, if not all organizations. Granting access to data to your users is just as important as restricting data. Without the correct access to the necessary information, employees will not be able to accomplish their day to day tasks in the course of their jobs. Roles are utilized in Remedyforce to enforce what data can be accessed in a hierarchical fashion, with the top of the hierarchy granted access to the highest level of data and restricting access as you move down in the hierarchy.

Permission Sets

When there is a need to grant specific individuals in your organization greater levels of access to your applications, permission sets can be created that can be applied, either temporarily or permanently, to those individuals. This provides the ability to modify a user’s level of access without the need to manage numerous profiles within the Salesforce Platform. Permission sets are similarly configured the same as Profiles.

Copyright BMC Software, Inc. 2015

User Creation

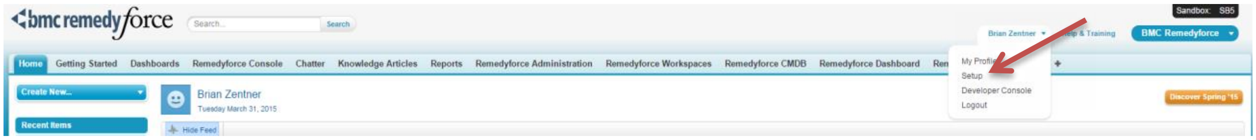
The creation of users can be a manual or automated process. Depending on an organization's needs, level of internal support resources, and security requirements, there are multiple ways to accomplish user creation.

Manual Creation

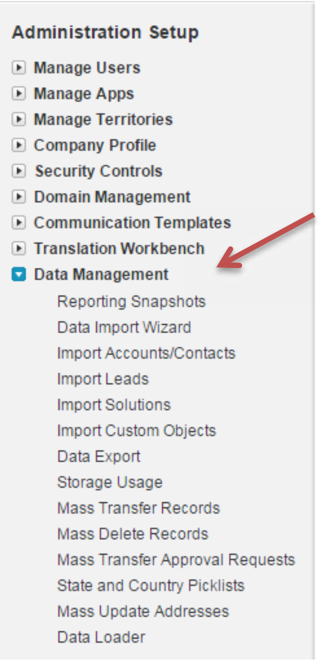
The simplest, but most time intensive way to create and maintain user accounts. This path would require all new users, all modifications to user information, and all deactivations for users to be managed by a Remedyforce Administrator. This can cause delays as this process could cause delays until the Remedyforce Administrator makes the updates to the application. Also this process leaves the potential for human error in the creation or modification to user accounts. Salesforce's Data Loader tool can be leveraged to do the initial insert of users but is only useful for a one time insert by importing a list of users from a CSV file. Remedyforce Administrators would still need to manually update the user accounts for future changes and deactivations.

As some companies do not have clean Active Directory structures defined, or all of their users are not contained in Active Directory, this is a good method to maintaining users in Remedyforce.

To install the Data Loader application, log in to your Salesforce org and click on Setup from the dropdown under your name at the top of the page.

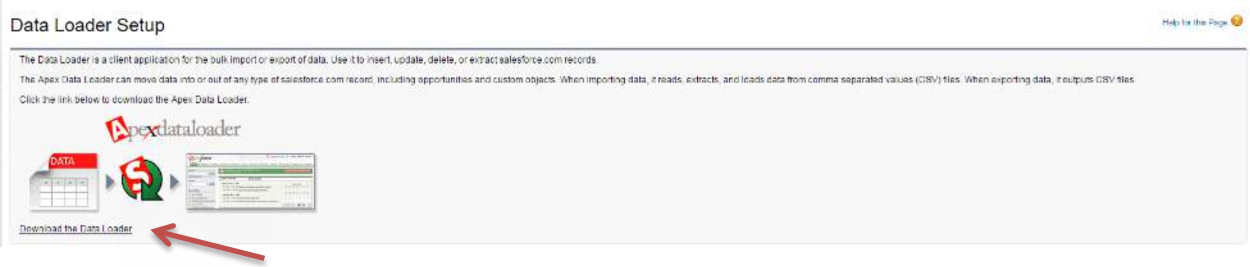


Then select Data Management from the Administration Setup section on the left and select Data Loader.



Then install Data Loader by clicking Download Data Loader.

Copyright BMC Software, Inc. 2015



Data Loader Setup

The Data Loader is a client application for the bulk import or export of data. Use it to insert, update, delete, or extract salesforce.com records.

The Apex Data Loader can move data into or out of any type of salesforce.com record, including opportunities and custom objects. When importing data, it reads, extracts, and loads data from comma separated values (CSV) files. When exporting data, it outputs CSV files.

Click the link below to download the Apex Data Loader.

Download the Data Loader

Many resources are available at Salesforce.com to assist you with data loader and manual user creation.

Data Loader: https://developer.salesforce.com/page/Data_Loader

User upload using Data Loader: https://help.salesforce.com/apex/HTViewSolution?id=000007571&language=en_US

Single Sign-On Provider

A Single Sign-On provider, or SSO, can implement a solution that would allow for real-time integration of Remedyforce to a company's Active Directory environment. This solution provides not only an integration path, but could also allow users to log into Remedyforce without the need to enter their username and password credentials. Also, the password change requirements for a company would then only need to be maintained in Active Directory. This reduces administrative overhead the need for users to maintain different passwords across multiple applications.

Integrations with a SSO typically only require a couple of hours to complete with the assistance of a technical representative of the SSO organization. The SSO would also provide continuing technical support for the integration after the initial configuration is completed. This would be a good option for those with a clean Active Directory environment, but limited resources to manage authentication administration.

OneLogin, a Single Sign On provider, is a BMC Software recommended partner that provides Microsoft Active Directory integrations to a customer's environment. They provide basic plans to Remedyforce customers ***at no charge*** that include capabilities for both real-time user provisioning and SSO. The details of OneLogin's offering can be viewed at https://www.onelogin.com/partners/app-partners/remedyforce-sso.

Pentaho Data Integration

Leveraging the power of an Extract, Transform, and Load tool, or ETL, customers can copy user data from their Active Directory structures directly into the Salesforce Platform to grant user access to the Remedyforce application. The recommended application to achieve this is Pentaho's Data Integration application, available ***at no charge*** from the company's website. BMC Software provides pre-configured packages that require little modification to become functional in your environment.

Pentaho displays the flow of data in a graphical interface that is easy to manipulate and provides many tools to leverage that provide customers the capability to build data flows ranging from very simple to very complex. Pentaho allows for the testing of your solution in a sandbox environment to ensure data accuracy and error checking. Once configured and data is verified, the Pentaho package is scheduled to run at an interval determined by the customer based on the company's needs. Log files are generated for review to determine successes and failures that occurred during the data import.

Pentaho integration to Active Directory is a good choice for companies with a clean but potentially more complex Active Directory structure. Through the use of LDAP queries, more diverse structures are able to be supported. Pentaho does require more administrative oversight than a SSO provider solution would, but eliminates the burden of maintaining user accounts manually. This solution would also benefit from a company having internal resources that are familiar with Active Directory and maintaining an ETL solution

Many resources on Pentaho are available on the BMC Communities website. Please login at https://communities.bmc.com to review.

Copyright BMC Software, Inc. 2015

Pentaho download: http://kettle.pentaho.com

LDAP Support Files

Using Permission Sets: https://communities.bmc.com/docs/DOC-32288
Not using Permission Sets: https://communities.bmc.com/docs/DOC-22547

Federated Authentication

Single Sign-On can also be achieved utilizing Federated Authentication with Security Assertion Markup Language (SAML). This allows integration with a company's Active Directory structure without the need to transfer data outside of the network, providing for a higher level of security. Federated Authentication is available to all Salesforce organizations but does require somewhat extensive knowledge in Salesforce and XML development. Similar to the services provided by an SSO provider, this integration is maintained solely internally and managed by a technical resource provided by the customer.

This solution is a good choice for companies that require SSO, high security, and the resources available internally to maintain the integration.

Please review documentation from Salesforce on the implementation of Federated Authentication using SAML.

Single Sign-On Implementation Guide
https://login.salesforce.com/help/pdfs/en/salesforce_single_sign_on.pdf

Single Sign-On with Force.com and Microsoft Active Directory Federation Services
https://developer.salesforce.com/page/Single_Sign-On_with_Force.com_and_Microsoft_Active_Directory_Federation_Services

Advantages / Disadvantages of Authentication/User Creation Options

Integration Type	Good Option For	Integration Type
Manual	Environments with no defined Active Directory Environments with a mix of users in Active Directory and users not in Active Directory Environments with fewer users to maintain	Manual
Single Sign On provider	Quick to implement Provides SSO and real-time provisioning Vendor support from SSO provider Minimal administrative overhead to manage once implemented	Single Sign On provider
Pentaho Data Integration	Can support a diverse Active Directory structure Data flows can be modified to meet each customer's unique needs Data remains inside of customer's organization Unlimited Active Directory attributes can be mapped	Pentaho Data Integration
Federated Authentication using SAML	Very secure Data remains inside of customer's organizations SSO capability	Federated Authentication using SAML

Copyright BMC Software, Inc. 2015

Considerations for User Creation and Authentication

User creation and authentication is a very important part of the Remedyforce configuration strategy. Utilizing the information above, a company must consider many factors to determine the best method and best fit for their organization. Some questions you may want to ask your team include:

Do you have a clean Active Directory Structure?

Is your organization's Active Directory structure well maintained and clearly defined? When integrating with Active Directory, it is very important to have a well-defined structure to ensure that users that will be created in Remedyforce have the correct permissions, correct geographic information, and should actually be allowed to authenticate to Remedyforce.

Do users have email addresses?

Salesforce requires all users to have email addresses. This is utilized to send users emails for password resets, communication between staff members and customers. This also serves as the key field for Pentaho integrations. If your users will not have valid email addresses, a field would need to be defined to map to for the account to be imported.

Does your company need to meet any security or compliance standards?

This could be one of the main deciding factors when you determine the best integration and authentication methods for your organization. If high security is required, you may not be able to take advantage of a SSO provider's offerings.

Do you have the internal resources with the knowledge to manage a more complex solution?

Comparatively, some solutions require a much higher level of technical resources than others. Please keep this in mind when you make the decision on the method you choose.

Where are you located?

Some organizations, depending on where they are based may be limited to certain SSO Providers, or require a specific form of authentication based on their country's laws or their organization's policies.

Do you have more than one Salesforce org?

Usernames in Salesforce are typically based on the email address of the user and are unique in that Salesforce org as well as all other orgs. If your company already has a Salesforce org that is in production and your Remedyforce implementation will be hosted on a different org, you will need to consider how you are going to generate a username for your users in your Remedyforce environment. Some solutions provide better support for this than others.

In Summary

In conclusion, the selection of a user creation and authentication method is a very important part of your Remedyforce configuration planning. A good understanding of the differences and requirements needed for all the solutions available is key for a successful implementation. If Active Directory integrations to Remedyforce is a future initiative, leverage your Active Directory environment, and ensure it is cleansed of unused data and structured well. Know the security and compliance requirements for your company and any restrictions that could be imposed by your government.

BMC Remedyforce has an extremely active user community where you can get answers to additional questions on this topic. We encourage you to take a look at bmc.com/communities.

Copyright BMC Software, Inc. 2015

BMC delivers software solutions that help IT transform digital enterprises for the ultimate competitive business advantage. We have worked with thousands of leading companies to create and deliver powerful IT management services. From mainframe to cloud to mobile, we pair high-speed digital innovation with robust IT industrialization—allowing our customers to provide amazing user experiences with optimized IT performance, cost, compliance, and productivity. We believe that technology is the heart of every business, and that IT drives business to the digital age.

BMC – Bring IT to Life.