Cloud security features whitepaper

Sage CRM

Document version 2016

Table of Contents

1.0 Introduction

Establishing a secure Sage CRM system is paramount to safeguarding your return on investment. Sage realises the importance of data security and takes this responsibility extremely seriously. We utilise some of the most advanced technology for Internet security available today including the use of industry standard Secure Socket Layer (SSL) technology to ensure all communications to and from the Sage CRM Cloud platform is encrypted.

This whitepaper reviews the built-in features of Sage CRM which support the wide range of security requirements which our customers demand in the Cloud. All aspects of platform security are built in for Cloud customers. Please refer to the Data centre & Platform Security Whitepaper for more information.

2.0 Essentials and Professional Editions

Sage CRM applies safeguards on multiple fronts within the application. The **Essentials** edition provides a solid set of security features aimed to comprehensively meet the demands of any organization operating in the Cloud:

- **Securing user access**. User authentication and password set- up, company team restrictions, and differentiated levels of Administration access all ensure secure user access to Sage CRM.
- **Field Level Security**. Set up field-by-field read/write access.

The **Professional** edition provides all the security features included in the Essentials edition with more advanced data segmentation and workflow capabilities often required by larger organizations:

- **Defining security profiles**. Define security profiles for View/Insert/Update/Delete rights across primary entities.
- Segmenting data access. Segment data access with hierarchical territory management.
- **Running workflows**. Guide users through pre-defined access points with detailed automated change tracking.

2.1 Further reading

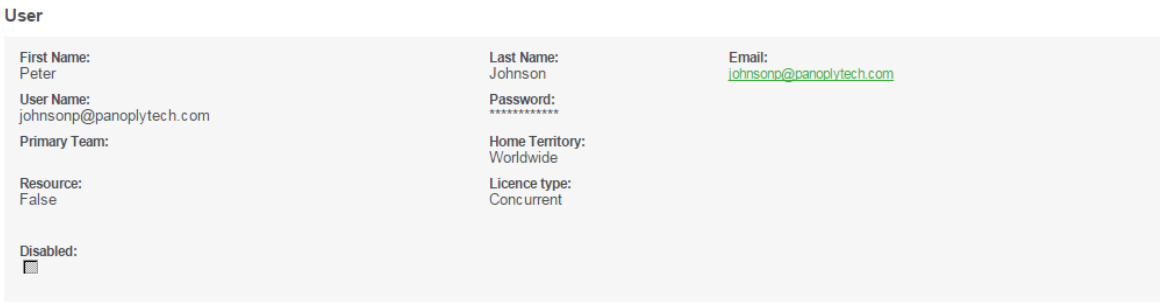
Scalability and Security in the Cloud, read the Rackspace Hybrid Hosting case study

Data centre & Platform Security Whitepaper available on http://trust.sagecrm.com

Sage CRM Editions Matrix

3.0 Securing User Access

A user requires a logon ID and password to access the system.



User authentication and password setup

3.1 User setup

A user's password is encrypted both within the system and in the database for maximum security. The System Administrator can change, but not view, a user's existing password.

3.2 Company Team restrictions

Rights to view “sensitive” tabs, such as Opportunities and Cases, can be restricted for individual users depending on company team membership. This means that if you have not been assigned to work on an account via the Company Team tab, you may not view or update information in “sensitive” tabs.

3.3 Differentiated levels of Administration access

User Administration rights can be set to differentiated levels of complexity. There are three basic levels: No Admin Rights, Info Manager, and System Admin. The Info Manager level can be allocated further specific rights. For example, in larger organizations, a number of power users can be given the ability to perform some specific system administration tasks – such as uploading templates, or maintaining currency conversion rates – without opening up the whole of the Administration area to them.

Info Managers also embody a more general concept of a power user. For example, setting the Administration field on a user to Info Manager automatically gives a user access to Marketing, and lets them edit Interactive Dashboard templates.

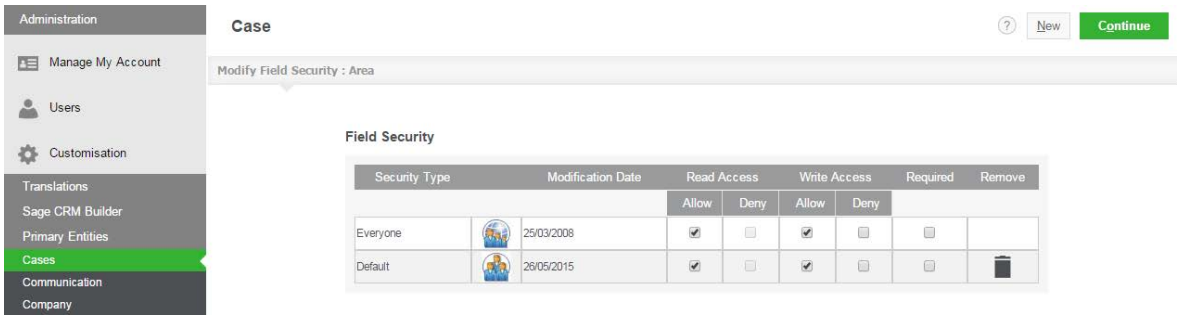
3.4 Further reading

Company Team related field descriptions in Security Fields help topic

Levels of Administration access (Info Manager) help topic

4.0 Setting up Field Level Security

Field security allows System Administrators to define how users can access the fields associated with a screen. For example, it is possible to make a field invisible to some users, allow others to view the contents of the field but not to change them, and to grant others both read and write access. In addition, it is also possible to make it mandatory for the user to enter a value in the field before submitting the form.



Field Level Security

This field security can be supplemented by System Administrators with JavaScript skills, who can add code in the scripting boxes available through the Screens tab when customizing an entity.

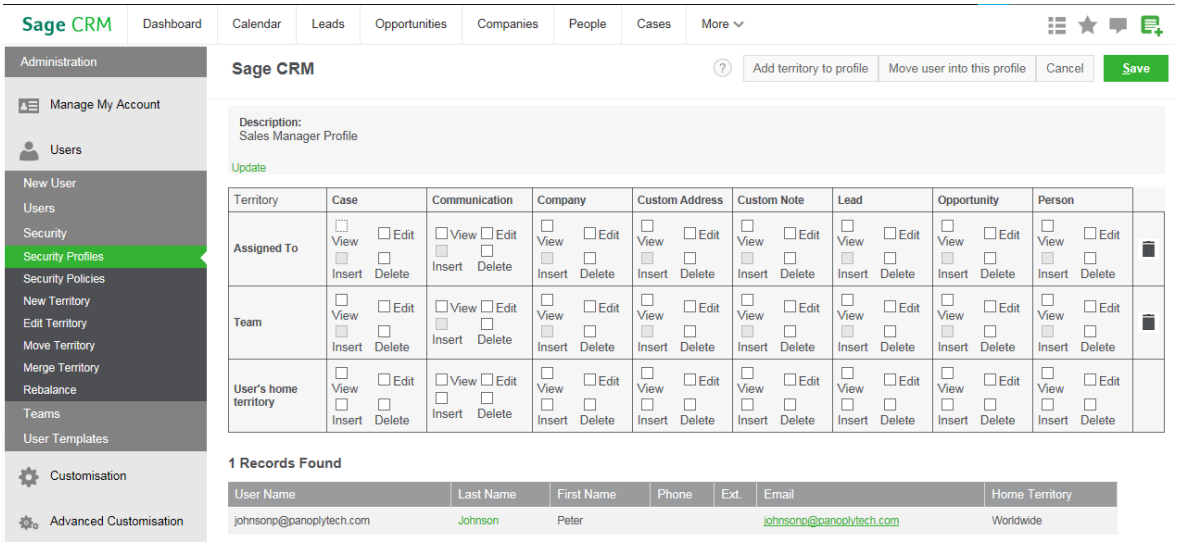
Field Security can be set for Everyone (all users), an individual user, a team, a security profile, or a combination of these security types.

4.1 Further reading

Field Level Security help topic

5.0 Defining Security Profiles

A security profile is a way of grouping users when defining access rights (View, Update, Insert, Delete).



Security Profile

For example, you can create a profile called Sales. Within the profile you define the rights to View, Update, and Insert Companies, People, Communications and Opportunities, but View-only rights to Cases. This profile can then be assigned to all sales users, rather than setting up individual rights per user. Any changes that need to be made to the profile will automatically apply to all users assigned to the Sales profile.

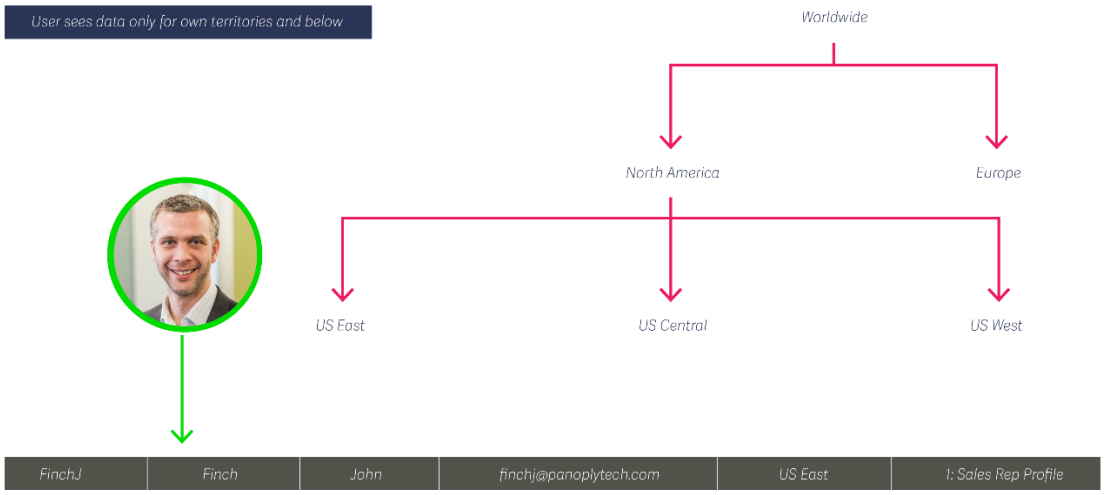
5.1 Further reading

Security Profiles help topic

6.0 Segmenting Data Access

6.1 Territory management

In addition to security profiles, you can also further divide user rights by territory. For example, you may want users in the Europe territory to view all Opportunities within the USA territory, but not to be able to update them.

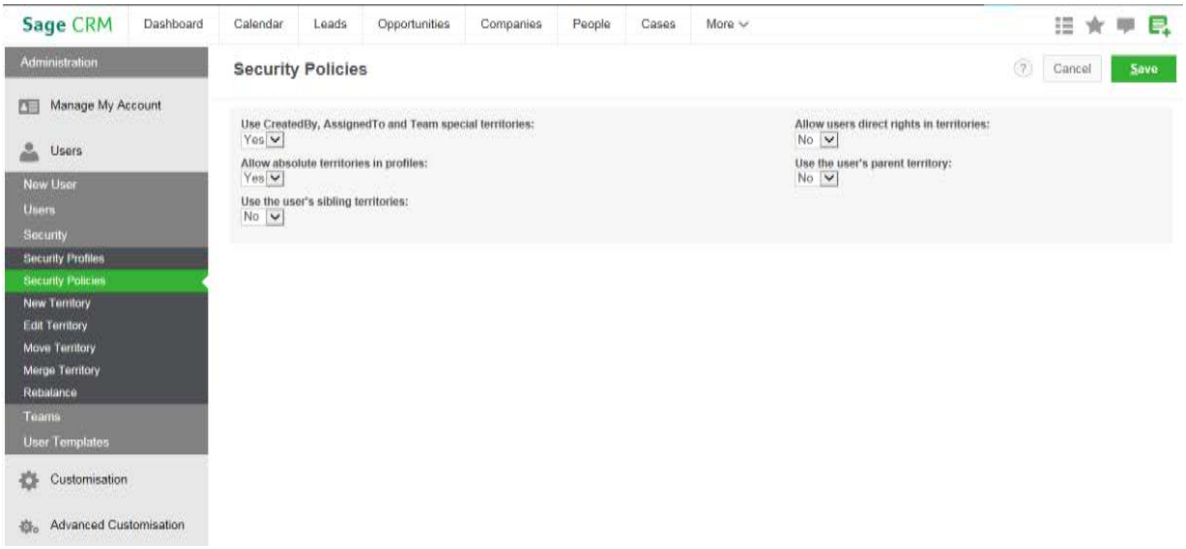


Territory Management

Territories act as a silent filter over existing security profiles. In other words, if you do not have View access rights to Opportunities in your profile, you do not see any Opportunities, no matter what territory they are in. The "silent filter" of territories influences all areas of CRM. This includes, searching, reporting, and groups generation.

6.2 Security Policies

Complex inter-territory security rights and exception handling are also catered for using Security Policies.



Security policies

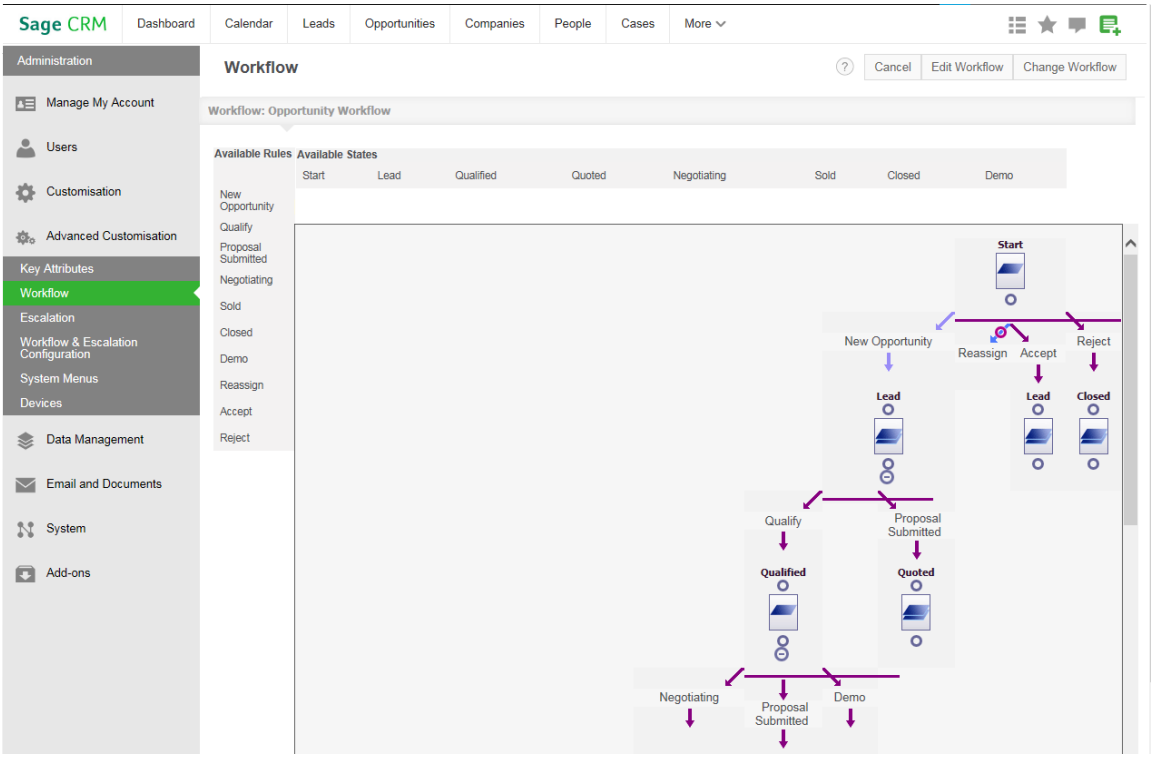
Security Policies allow the System Administrator to set up additional security rights. When settings within the Security Policies page are enabled, additional options are available in the Security Profiles page. The security policies act as logical "OR"s to the existing Profile and Default Territory settings.

6.3 Further reading

Territory Management help topic
Security Policies help topic

7.0 Running Workflows

The workflow functionality lets a user with system administrator rights set up predefined rules and actions to suit your organization's business processes.

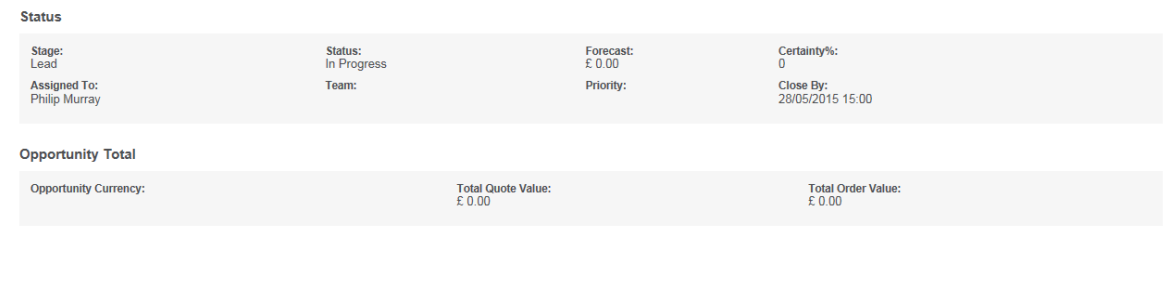


Defining a Workflow

For example, a workflow rule can be applied to opportunities to automatically generate a follow-up call for the user every time a quotation is sent out. Or, a workflow rule can be applied to cases to send an e-mail to the customer service supervisor if a case remains at a stage of "Investigating" for more than twenty-four hours.

7.1 Pre-defined workflow actions

If you have already been working with leads, opportunities, cases, and solutions without workflow, you will have used the Progress button to manually "progress" the entity to the next stage within the lead, sales, or customer service cycle. Once workflow is activated, this button is no longer available. It is replaced with bullets appearing under a common heading Actions.

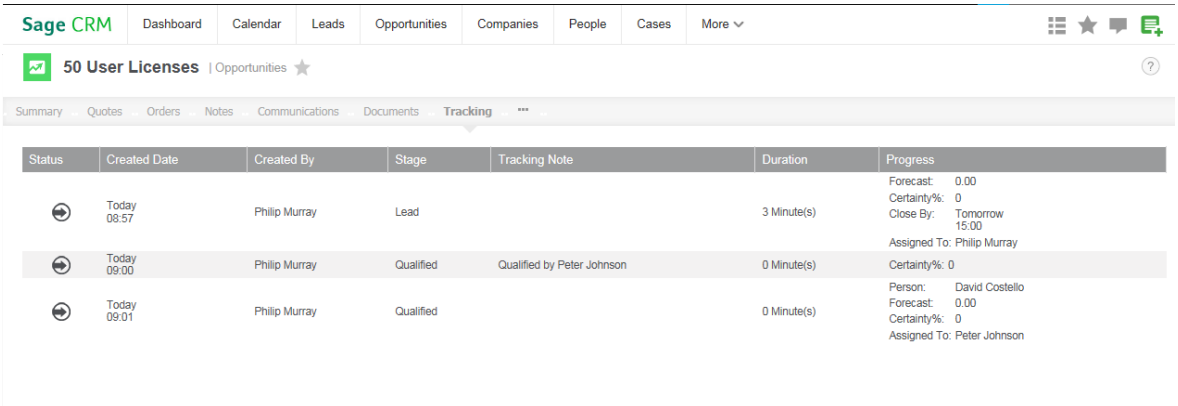


Workflow Actions

These actions are set up by the system administrator to steer the user through the predefined business processes. Selecting one of these actions can prompt the user to perform an activity, such as gathering further information. It can also trigger events which are not immediately apparent to the user, for example, sending an SMS notification to the Account Manager.

7.2 Automated workflow tracking

Every change or progression to a record through the workflow process is recorded in the Tracking tab.



Workflow Tracking tab

The Duration column shows how long, for example, the opportunity has spent at each stage of the qualification process. The duration takes into account the business calendar defined by the System Administrator.

7.3 Further reading

Workflow Customization help topic