RIMS IT Setup Items

RIMS (Real Estate Information Management System) is an outsourced software application that manages the workflow of internal personnel and external contractors as they collaborate to perform real estate due diligence tasks. LightBox Holdings, L.P. ("LightBox") is the vendor that provides the RIMS application and hosts the ExactBid application servers.

RIMS informs users of key events via an email notification system implemented using its own email servers. Users access RIMS via the internet with standard web browsers.

This document describes how the institution's network and the users' browsers must be configured to be fully compatible with RIMS functionality.
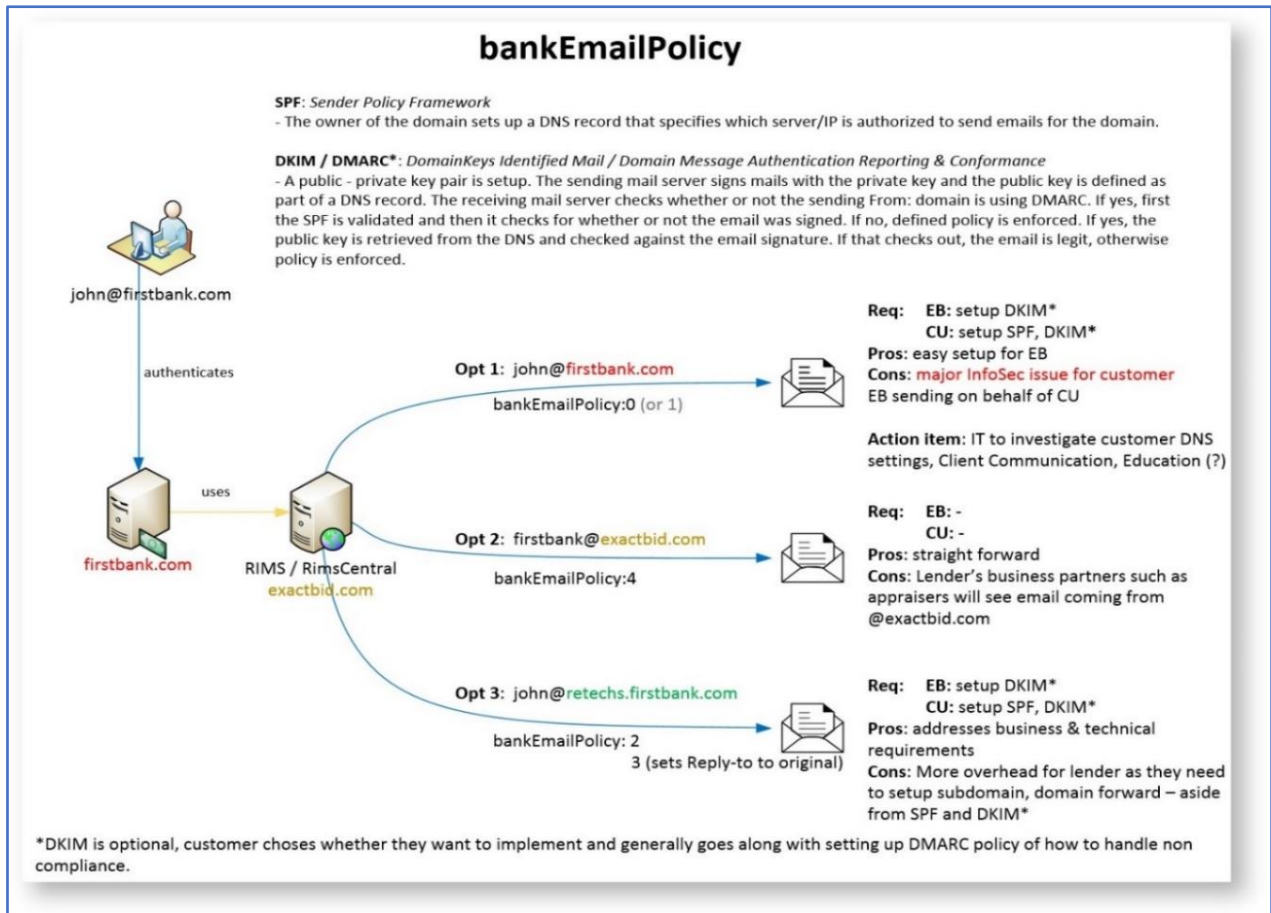
ACCOMMODATING RIMS EMAIL NOTICES

The RIMS application utilizes email notices to internal and external users of RIMS to enhance communication and ensure participation by the appropriate individuals. Default FROM addresses for these notices take the form rimsOrganizationname@exactbid.com where 'Organizationname' is your institution's name or recognizable alternative.

For select communications, the user's email address is utilized as the FROM address. In these cases, the user is also a recipient of the notice to ensure a message history is available. Some institutions block this type of mail by default. Please ensure that this type of email (where FROM and TO are the same within the organization's domain) is permitted.

Email from RIMS can be sent in one of two different ways:

1) Option 1: Email from RIMS is sent from an ExactBid email server owned by LightBox and utilizes a custom, dedicated email address for your organization. For example, if your organization were "Second Bank," LightBox IT would set up an email address similar to secondbank@exactbid.com and every email generated from RIMS to the identified recipient(s) would appear to be coming from secondbank@exactbid.com. You can also specify the default reply-to address: e.g. "Reply-To: firstname.lastname@secondbank.com". This configuration is very straightforward and does not require involvement from your organization's IT Department.

2) Option 2: RIMS can be configured to send email on behalf of your organization with the sender email address showing your organization's domain. For example, if the organization name is "Second Bank" and the domain name is secondbank.com, set the "FROM" email address to firstname.lastname@secondbank.com. If this is the option you would like to

select, then various requirements must be met for LightBox to send email on behalf of your domain. One of the prerequisites is to set up a specific SPF entry for the ExactBid email server's IP address to be authorized to send email on behalf of your organization's domain. Other settings to be determined with your IT Department.

bankEmailPolicy

SPF: *Sender Policy Framework*
- The owner of the domain sets up a DNS record that specifies which server/IP is authorized to send emails for the domain.

DKIM / DMARC*: *DomainKeys Identified Mail / Domain Message Authentication Reporting & Conformance*
- A public - private key pair is setup. The sending mail server signs mails with the private key and the public key is defined as part of a DNS record. The receiving mail server checks whether or not the sending From: domain is using DMARC. If yes, first the SPF is validated and then it checks for whether or not the email was signed. If no, defined policy is enforced. If yes, the public key is retrieved from the DNS and checked against the email signature. If that checks out, the email is legit, otherwise policy is enforced.

john@firstbank.com

authenticates

uses

firstbank.com

RIMS / RimsCentral
exactbid.com

Opt 1: john@firstbank.com
bankEmailPolicy:0 (or 1)

Opt 2: firstbank@exactbid.com
bankEmailPolicy:4

Opt 3: john@retechs.firstbank.com
bankEmailPolicy: 2
3 (sets Reply-to to original)

Req: EB: setup DKIM*
CU: setup SPF, DKIM*
Pros: easy setup for EB
Cons: major InfoSec issue for customer
EB sending on behalf of CU

Action item: IT to investigate customer DNS settings, Client Communication, Education (?)

Req: EB: -
CU: -
Pros: straight forward
Cons: Lender's business partners such as appraisers will see email coming from @exactbid.com

Req: EB: setup DKIM*
CU: setup SPF, DKIM*
Pros: addresses business & technical requirements
Cons: More overhead for lender as they need to setup subdomain, domain forward – aside from SPF and DKIM*

*DKIM is optional, customer choses whether they want to implement and generally goes along with setting up DMARC policy of how to handle non compliance.

In 2025, LightBox will be moving from IceWarp to SENDGRID for email. Below is an updated image of how the policies will work after this change is completed.

Bank Email Policy
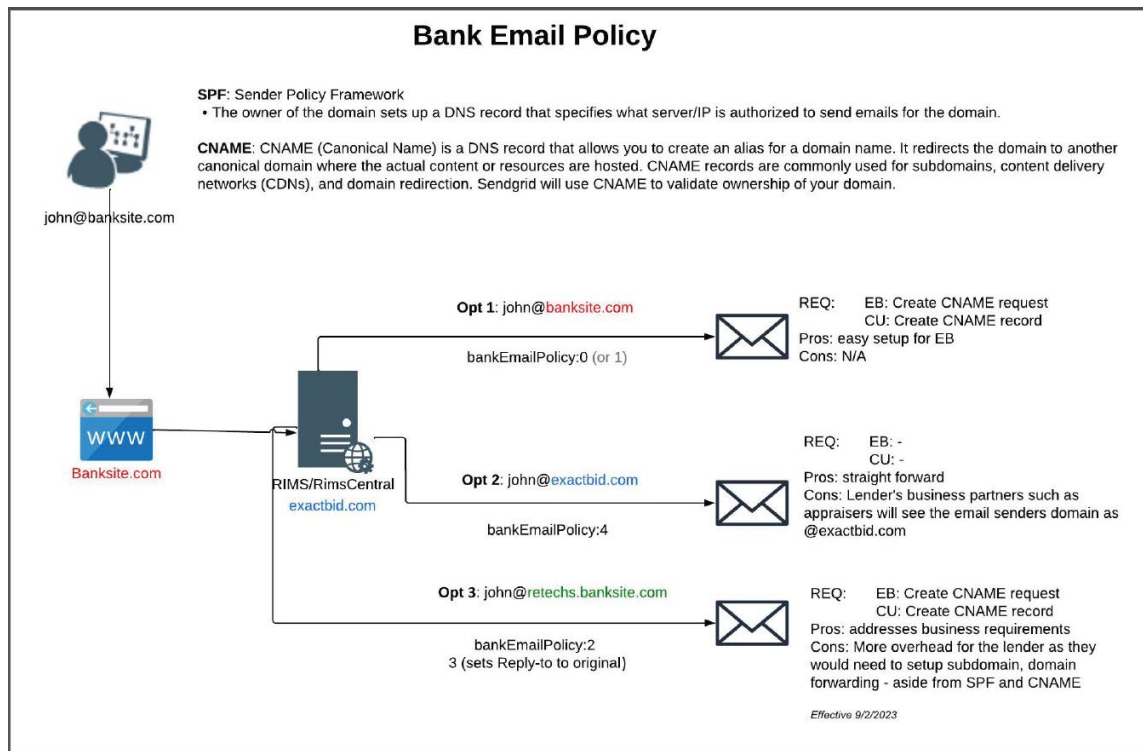
Once you determine whether Option 1 or Option 2 suits your institution's needs, please confirm your decision with RIMS Customer Support. If you decide that Option 2 is preferable, please provide contact information for an individual on your IT Team that is familiar with email and DNS – SPF configuration so we can schedule time to implement the settings and configurations. Please provide this information at your earliest convenience, as there can be up to 2 weeks of lead time required to get certain DNS configurations approved and promoted.

Additionally, if your organization uses whitelists for bypassing email filters and ensuring email delivery, the following ExactBid email servers should be added to the whitelist:

- rimsmail.exactbid.com – **34.215.165.231,** 23.20.119.18 (primary – production site email)
- maildev.exactbid.com – 44.209.122.53, 54.235.79.89 (primary – development/UAT site email)

BROWSER SETUP FOR RIMS COMPATIBILITY

Browsers can be configured in a standard way. However, there are a few items to check.

On the **Internet Options/General** tab, click on the **Settings** button in the **Browsing History** section. Under **Check for newer versions of stored pages**, check *Every time I visit the webpage or automatically*.

On the **Security** tab, click **Custom Level**. *Allow META REFRESH* should be enabled.

On the **Privacy** tab, it is best to choose some settings that allow cookies from exactbid.com. Choosing **Medium High** will work, or you can explicitly accept cookies from exactbid.com.

On the **Security** tab, click on the **Trusted Sites** option and add the following URLS:
- https://reportx8.exactbid.com
- https://rimsreportsadhocproxy-uat.exactbid.com

You must also add your organization's RIMS site URLs to Trusted Sites. Add both the production environment and the UAT environment URLs. Example:
- https://ExampleBank.exactbid.com
- https://ExampleBank-uat.exactbid.com

This will ensure RIMS Users will have access to our AdHoc Reporting tool to build customer reports.

Finally, RIMS uses pop-ups to convey certain on-demand information to users. Accordingly, the RIMS application and specifically the exactbid.com domain must be marked as "safe," "cleared," or "whitelisted" regarding any pop-up blockers employed by the users. Alternatively, all users must manually turn off their pop-up blockers when accessing RIMS.

RIMS LOGIN – USER AUTHENTICATION

RIMS User Login and Authentication can be managed in two ways:

1) Provide your login credentials and password settings, including the frequency of password resets, to RIMS Customer Support. We will use the settings you provide to configure your RIMS Login process.

2) RIMS does support SSO (Single Sign On) and centralized user account management through your domain with SAML. If your organization would like to implement SAML for user account management and access control for RIMS, please provide contact information for a member of your Domain Trust Management Team so that IT and/or Development representatives of both organizations can work directly to get SAML configuration requirements identified and set up for a timely deployment of RIMS within your organization. SSO can authenticate against a user's email address or an Import User ID value such as Employee ID.

3) Please contact your Customer Success Manager for our Fact Sheet & Set Up Documentation.

IP RESTRICTIONS

RIMS can restrict user access to specified location through IP restriction settings. A provided list of IP addresses for proxy servers can be utilized to verify that the user attempting to access RIMS is accessing the application from within the customer's network.

IP restrictions ensure that former employees cannot access RIMS once their access to network resources is terminated. For current employees, access can be made from any physical location provided the connection is made via a VPN-connected device or a workstation connected to the local area network.

If your organization would like to implement IP restriction, please contact RIMS Customer Support. IP restriction can also be restricted by user type. Your organization will need to provide your list of proxy server IP addresses or address ranges if this feature is to be enabled.

If you have any questions, please contact:
RIMS Customer Support
866-319-7467
support@exactbid.com