TIBCO Slingshot

Quick Start Guide

Software Release 1.9.4
August 2015

Two-Second Advantage®

TIBCO™

Important Information

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENT IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE OR IF THERE IS NO SUCH SOFTWARE LICENSE AGREEMENT OR CLICKWRAP END USER LICENSE AGREEMENT, THE LICENSE(S) LOCATED IN THE “LICENSE” FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

This document contains confidential information that is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of TIBCO Software Inc.

TIBCO, The Power of Now, Two-Second Advantage, TIBCO Managed File Transfer, TIBCO Managed File Transfer Command Center, TIBCO Managed File Transfer Internet Server, TIBCO Managed File Transfer Platform Server, TIBCO Managed File Transfer Platform Server Agent, Edge Server, RocketStream Accelerator, and Slingshot are either registered trademarks or trademarks of TIBCO Software Inc. or its subsidiaries in the United States and/or other countries.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only.

THIS SOFTWARE MAY BE AVAILABLE ON MULTIPLE OPERATING SYSTEMS. HOWEVER, NOT ALL OPERATING SYSTEM PLATFORMS FOR A SPECIFIC SOFTWARE VERSION ARE RELEASED AT THE SAME TIME.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

TIBCO® Managed File Transfer Internet Server with RocketStream® Accelerator is entitled TIBCO® Managed File Transfer Internet Server in certain other product documentation and in user interfaces of the product.

Copyright ©2003-2015 TIBCO Software Inc. ALL RIGHTS RESERVED.

TIBCO Software Inc. Confidential Information

Getting Started with Slingshot

This guide has been developed to walk you through the steps necessary to configure Slingshot for the first time. The steps discussed are required before the system can begin sending and receiving files.

To access the Slingshot Administrator screens copy and edit the following URL to connect to your system:

Slingshot Administrator URL format:

https://[DNS_HostName]:[httpsPort]/[context]/control?view=view/admin/start.jsp

To send files after the system has been configured, copy and edit the following URL to connect to your system:

Slingshot Send Files URL format:

https://[DNS_HostName]:[httpsPort]/[context]/control?view=am/start.jsp

Steps to follow to configure Slingshot:

Configure Slingshot Display Name
Configure Slingshot and the Vault Server
Defining Slingshot Users
Slingshot Web Browser Interface
Slingshot Outlook Plug-in Install

Additional Configurations:

Defining a MFT Platform Server
Slingshot Reports
Using PGP with Slingshot
More on Slingshot Assigned Rights
Disable Slingshot Plug-in

Configure Slingshot Display Name

Slingshot can be installed on a single server as well as on multiple servers within a network using different servers for authentication purposes. For the single server environment you can use the Display Name field to hold for instance your company name (default value). Otherwise in the multiple server environments this field can hold for instance your server name in order to help associate end users with their home server. The information configured in this field will be displayed at the top of the Slingshot Administration web pages (notice the top line in Figure 1) and the Slingshot Web Browser Interface web pages (See Figure 2).

Warning: We strongly suggest that the Email URL be configured with an IP name (DNS Name). This URL is being referenced in emails sent out by Slingshot. If a change to the server IP address is ever necessary, old Slingshot emails will become inaccessible unless a DNS name is being used. The Email URL is first configured during the install of Slingshot in Step 4.

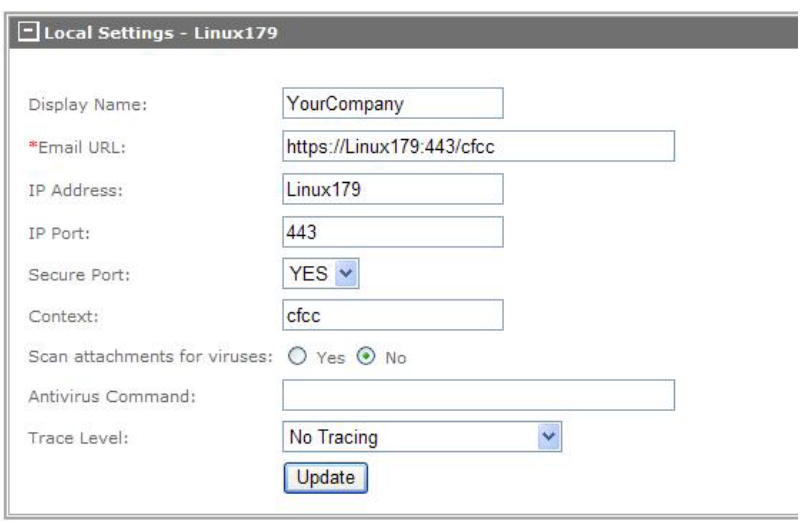

Figure 1

Figure 2

▲ Back to Top

Configure Slingshot and the Vault Server

You are now ready to configure Slingshot. Within Slingshot's Configurations is a Vault Server. This server is responsible for storing all the file attachments that were uploaded Slingshot and have expired.

Navigate to **Management > Slingshot > Configuration**

We will discuss the configurations by sections. The first section is the *Email Settings* Section. See Figure 3 below. Enter your Email Host Name (IP can be used). If you do not define the Email Host Port it will default to port 25.

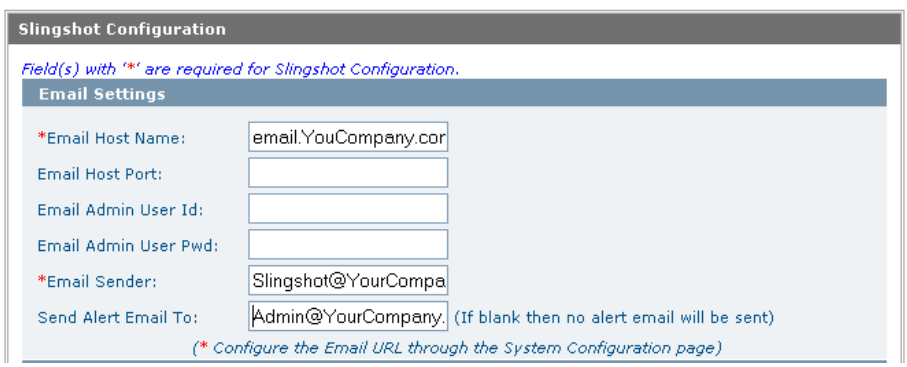

Figure 3

The second section is the *Repository Section*. See Figure 4 below:

Figure 4

This is the server that is responsible for holding all the file attachments that will be uploaded and downloaded by users when they are sending and receiving file attachments using either the Slingshot's Outlook Plug-in or the Web Browser Application. By default *LOCAL (the server in which Slingshot's software is installed on) is configured. If you have a Windows or Unix MFT Platform Server defined in your environment you may change the

repository server to use one of these machines. Only MFT Platform Servers will be in the drop down menu. (To read more about defining a MFT Platform Server see section defining a MFT Platform Server.)

In addition you must set the directory and file name where you would like the files stored on the repository server. For example: c:\SlingshotFiles.

Figure 5

In the *Settings for Users Created by Senders* section you are configuring how a Guest and Full User will be created when they are sent an email for the first time with Slingshot. You will read more about the Guest and Full Users later in Step 3.

Parameter	Definition	Default
User Visibility	Used only when assigning users to departments: Public - sees users in all departments in their Contacts list Private - only sees users in the same department in their Contacts list	Public
Internal E-mail Domains	Internal domains located within your production environment. Allowed Values: ALL, NONE, or 1 or more internal domains separated by a semi colon (;).	ALL
Create Users in External E-mail Domains	Any domains outside of your production environment.	Enabled
Initial User Status	Will a new user account that is created	Enabled

	be Enabled or Disabled	
Guest User Expiration	The amount of days a Guest user account will be active.	30
Guest User Reactivate	When enabled a Guest user account can be reactivated when a new Slingshot email is sent to them.	Disabled

Figure 6

The *Settings for Slingshot Outlook Plug-In* section is used to configuring Outlook rules to be followed when users are sending file attachments via Outlook.

Parameter	Definition
Rules	When a user clicks the Outlook Send button, do you want the Transfer Size Rule and Attachment Type Rule to be Enforced causing the user to have to send out the email with the file attachment using Slingshot or do you want to just suggest the user send the file attachment via Slingshot giving the user a choice?
Transfer Size Rule	An email with file attachment/s being sent via Outlook can not be any larger then this setting which when reached will result in the user being prompted with instructions to use Slingshot to send the email with the attachment/s.
Attachment Size Rule	An email with file attachment/s being sent via Outlook that contain particular file extensions will result in the user being prompted with instructions to use Slingshot to send the email with the attachment/s.

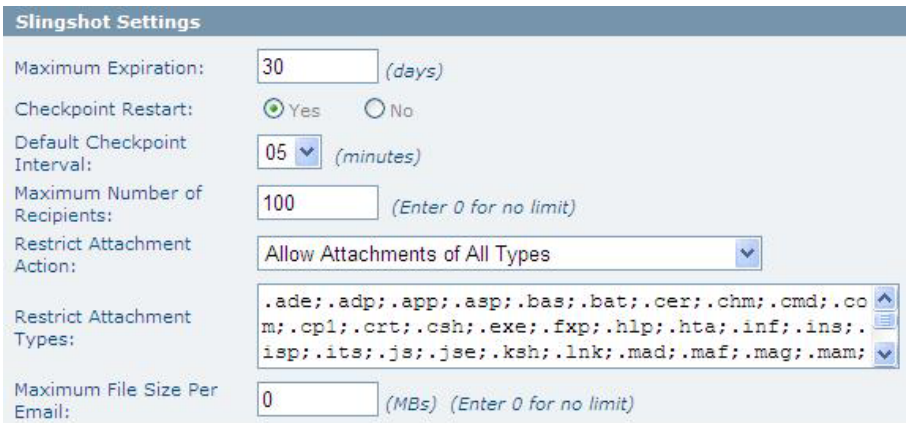

Figure 7

Figure 7 screen shot displays the default values for the email file attachments being sent via Slingshots Browser Interface, below is a brief description of the parameters:

Parameter	Definition
Maximum Expiration	How long before the email with the file attachment will expire.
Checkpoint Restart	A checkpoint is taken at the checkpoint Interval during an email file attachment transfer with the **Outlook plug-in** only to prevent the transfer from starting over should there be a loss of a connection of any kind.
Default Checkpoint Interval	Defines how often a checkpoint will be taken during a file transfer.
Maximum Number of Recipients	How many users would be permitted in one email sent in the combined To, CC and BCC fields.
Restrict Attachment Action	Use this to restrict a file with certain file extensions type from being sent.
Restrict Attachment Types	Enter the file extension types you would like to restrict from being sent.
Maximum File Size Per Email	The total Megabytes a file or a combination of files is allowed to be sent via Slingshot.

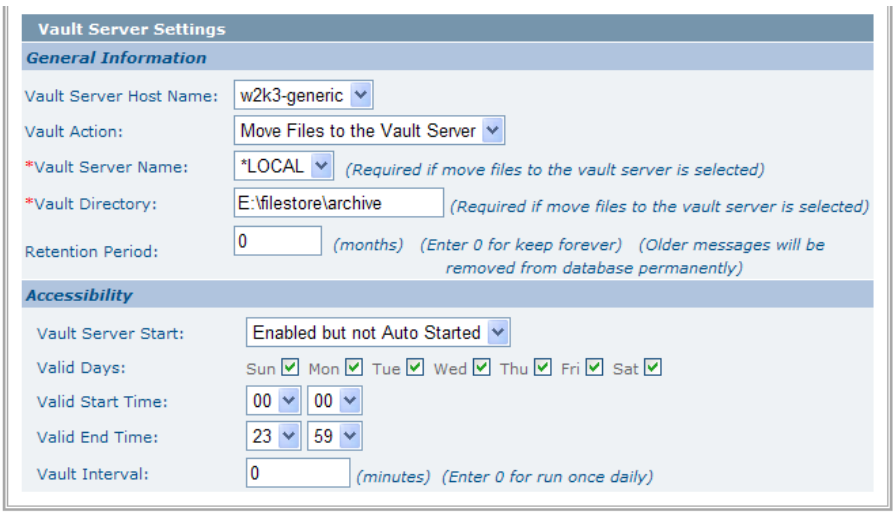

Figure 8

Figure 8 above is a screen shot of the *Vault Server Settings* section of Slingshot's Configurations page. The Vault Server stores the expired Slingshot email file attachments. What this means is when a Slingshot file attachment has expired (been flagged) the Vault Server will move the file attachment to a designated server when it sweeps through the file attachments sitting in the repository. Any change made to this section requires you to restart the Vault Server from **Management > Slingshot> Vault Server Status** web page.

By default the local Web server (*LOCAL) is the defined location for the Vault Server. A Windows or Unix MFT Platform Server may be used as a Vault server. You can further define your MFT Platform Server to use PGP whereby you are storing your files PGP encrypted. See Using PGP with Slingshot for further information on this type of configuration.
Files that are archived are still available to be downloaded by the sender as long as the file definition remains in the database. If the Retention Period has been set and been reached the file definition for a file transfer will be removed from the database and the file download will no longer be available.

Until the Valid Start Time has been reached the Vault Server will be in a sleep state.

If you do not make any changes to the Accessibility section and the service is running the Vault Server will run midnight every night by default.

Parameter	Definition
Vault Server Host Name	This is the server that will be responsible for running the Vault Server.
Vault Action	Do you want to move the files to the Vault Server or have the files deleted.
Vault Server Name	The name of the server being used to place the archived files.
Vault Directory	The directory where files will be placed on the Vault Server.
Retention Period	How long you want the file definition to remain in the database.
Vault Server Start	By default the Vault Server is set to be Enabled but Not Started. What this means is the Vault Server service must be started manually by going to the Vault Server Status web page and clicking on the Start button. Otherwise the following 2 other options are available: **Auto Start** – Service will start when your web server starts. **Disabled** – The service will be disabled at this time and no archiving will take place.
Valid Days	Days you want the Vault Server to run.
Valid Start Time	The time you want the Vault server to start to search for files.
Valid End Time	The time you want the Vault server to go to sleep.
Vault Interval	How often you would like the Vault Server to scan the repository during the Archiving time period.

▼Step 4

▲Back to Top

Defining Slingshot Users

There are three ways to create Slingshot Users:

1) If you are a Slingshot administrator you can log in and navigate to **Users > Add User** to add a user by following these steps: (See Figure 9)
    a. Set the User Id - It is recommended the User Id match the users email address.
    b. Set the Full Name of the user.
    c. Set the Password and Confirm the new password.
    d. Set the Slingshot Usage to ***Slingshot*** for the new user to be authorized to use the Slingshot Browser Interface or Outlook plug-in. (***Non-Slingshot*** is used more for administrators and they will not be able to use the Slingshot Browser Interface or Outlook plug-in).
    e. Set the User Type for the new user.
    f. Set an email address to be used for this user id. All ***Slingshot*** users must have an email address.
    g. Click on the Add button. (The only Assigned Right needed by a Slingshot user is the Transfer Right which is assigned by default. Read more about Slingshot rights in the More on Slingshot Assigned Rights section.)

Guest User	User can only send to users in the Contacts and cannot create a new user account or see other Guest user accounts.
Full User	Can create user accounts outside of the internal domain as long as this option is enabled in the Slingshot Configurations page.
Power User	Can create user accounts inside/outside of the internal domain.

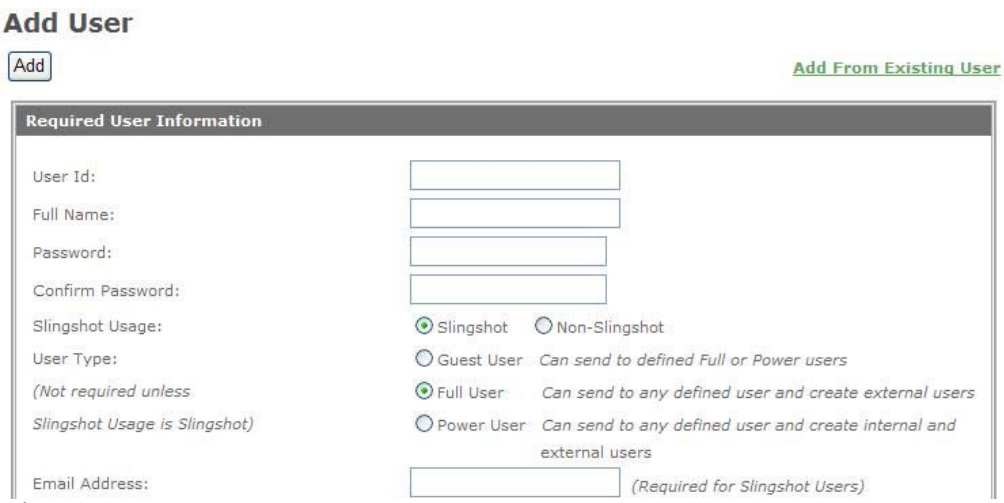

Figure 9

2) The second way to create a Slingshot user is to follow the steps in the first method and make a pre-existing Slingshot user or new user a Guest, Full or Power User.

   Then login to the Slingshot Browser Interface with the following URL filling in your DNS host name, https port, and context you are using:

   https://[DNS_HostName]:[httpsPort]/[context]/control?view=am/start.jsp

   or you can login to the Slingshot server using the Outlook Plug-in (The plug-in must be installed prior, See Step 6 and send a recipient(s) an email file attachment. Upon clicking the Send button you will be prompted with the following Create User window:

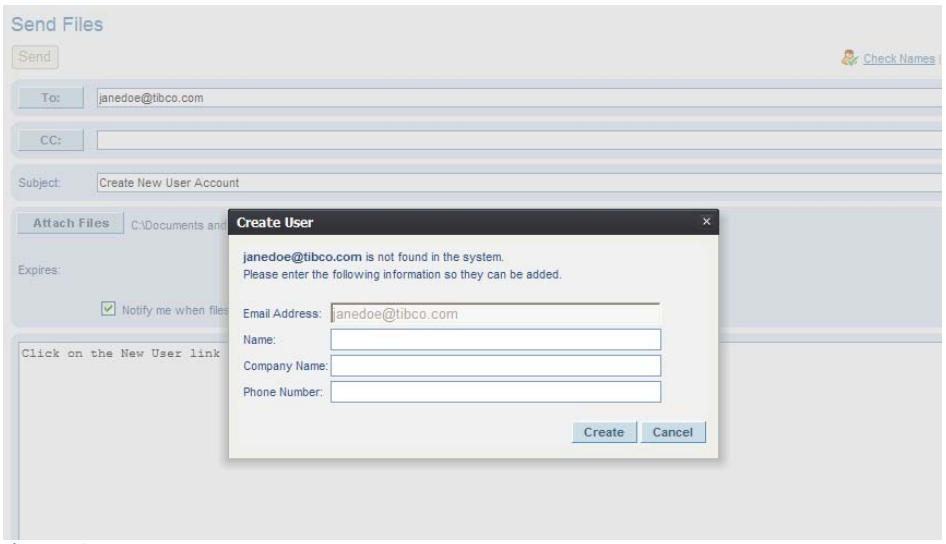

Figure 10

The sender will be prompted to enter the new user's Full Name (required), Company Name (optional), and the Phone Number (optional) for each new user they have configured in their email To, CC, or BCC fields. Once the Create button is clicked the new user's account(s) will be created and a "Welcome" email will be sent to each one.

3) The third way is to add users through an LDAP server (Microsoft Active Directory). For more information on this method read the LDAP section of the *Slingshot v1.9.2 Administrator Guide*.

▲Back to Top

Slingshot Web Browser Interface

Slingshot comes with 2 interfaces. We will discuss the Web Browser Interface here and the Outlook Plug-in in Step 6. If you have finished your configurations in Steps 1-5 a Slingshot user will be able to use the Slingshot Web Browser Interface.

To login to the Slingshot Browser Interface use the following URL filling in your DNS host name and https port you are using:

https://[DNS_HostName]:[httpsPort]/cfcc/control?view=am/start.jsp

You will see the following screen:

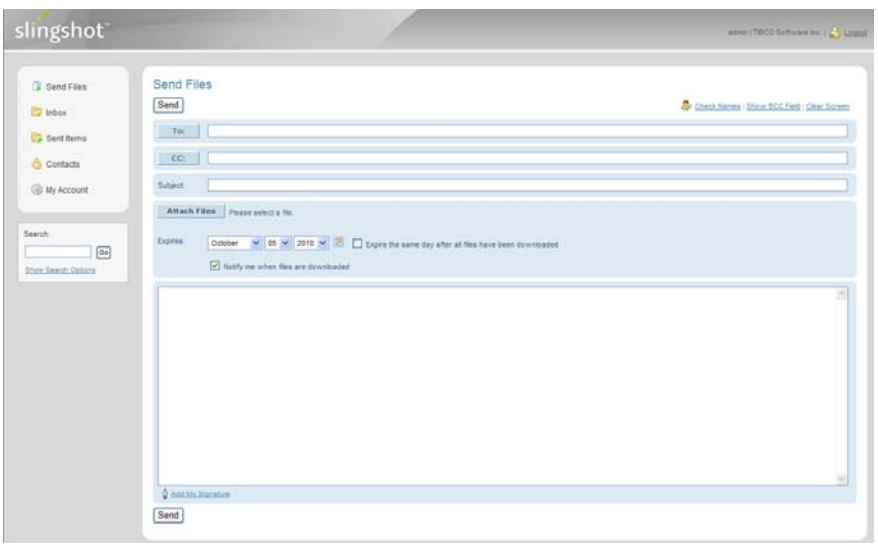

Figure 11

Note: If this is the first time the user is connecting he/she may have to set a new password.

▲Back to Top

Slingshot Outlook Plug-in Install

As mentioned in Step 5, Slingshot comes with 2 interfaces. We will now discuss Slingshot's second interface the Outlook Plug-in. This plug-in allows the end user to utilize all Slingshot's functions from the popular Microsoft Outlook Application.

By default, the Slingshot Plug-in installs with most Slingshot popup message windows disabled. You can enable Slingshot popup windows after installation by configuring the Transfer Tab on the Slingshot Options menu.

Pre-requisites:

1) ***Microsoft .NET Framework 2.0 or higher installed on their system.***
2) ***Visual Studio 2005 Tool for Office SE Runtime (Install provided for you, if needed.)***
3) ***Microsoft Office Primary Interop Assemblies (Install provided for you, if needed.)***

You can download the plug-in by using the following URL filling in your DNS host name and https port you are using:

https://[DNS_HostName]:[httpsPort]/[centext]/control?view=am/start.jsp&action=config.am

You will see a page similar to the one below:

Figure 12

As you can see from Figure 14 the end user can download the installation as an executable or in zip file format. The executable file can be used if you have the pre-requisites installed already or if you are upgrading from a prior Slingshot plug-in. Otherwise you will want to download the product contained in the zip file.

Simply click on the link of the one you would like to start the download.

*Note: For information on deploying the Slingshot Outlook Plug-in through your environment with a silent install refer to Slingshot installation guide for your web server. For our example below we will be using the **setup.exe** which is contained in the Slingshot Outlook Plug-in Zip File to install the plug-in product manually on a user's desktop for the first time.*

Running the install using the **setup.exe** is recommended because it will install everything the product needs except for the Microsoft .NET Framework (Please go to Microsoft.com to download v 2.0 or higher and follow Microsoft's instruction to install it). The first component it will look for is the Microsoft Visual Studio 2005 Tools for Office runtime. If this is not found you will be prompted to install it as seen in Figures 15 and 16 below:

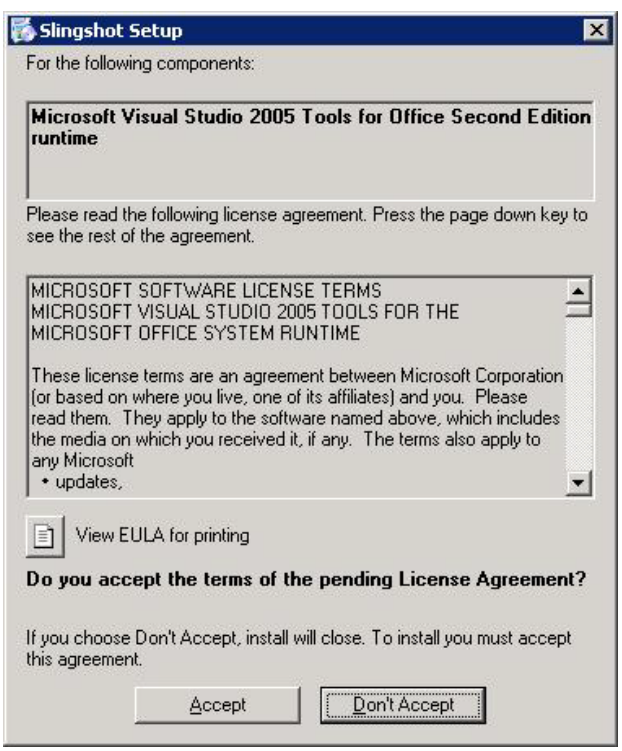

Figure 13

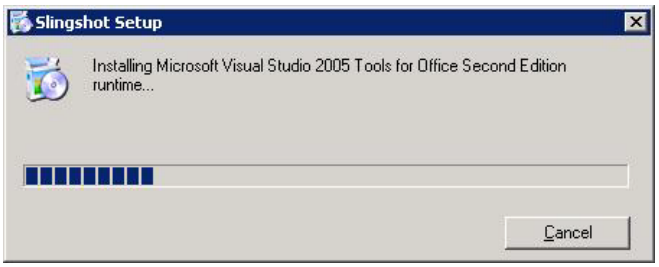

Figure 14

A reboot of the system may be required at this point.

Once you have installed the Microsoft runtime library and rebooted your system if required, double click on **Setup.exe** again. Slingshot will automatically which version of Outlook you are using. Based in the version of Outlook you are using the program will install a Primary Interop Assemblies program. This component is needed for the Slingshot Outlook plug-in interoperability between its .NET managed code and Microsoft Office COM libraries. We will then go on to install the Slingshot Outlook Plug-in as seen in Figures 15 – 20.

Figure 15

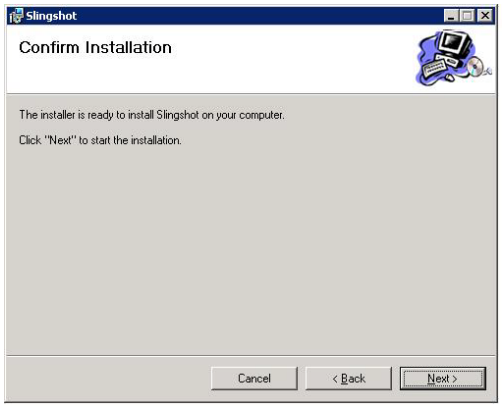

Figure 16

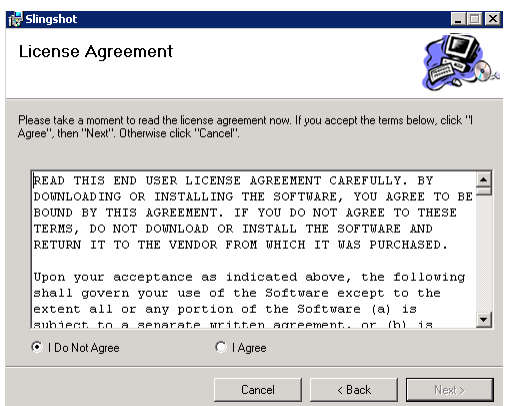

Figure 17

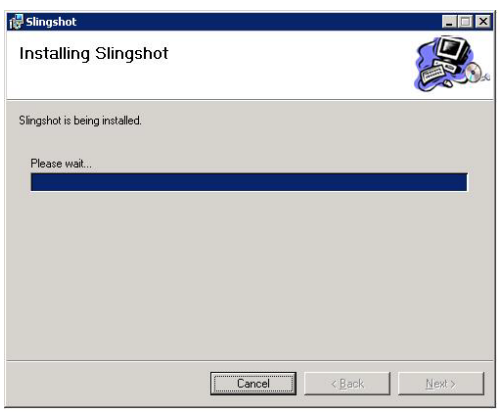

Figure 18

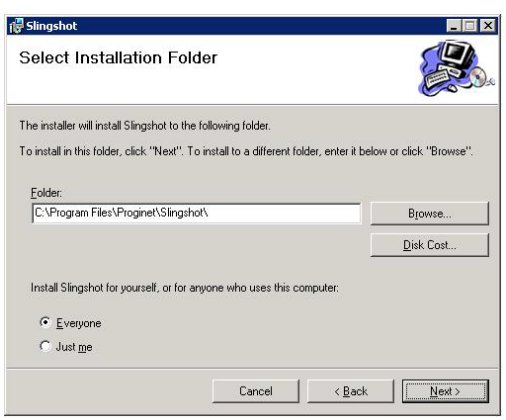

Figure 19

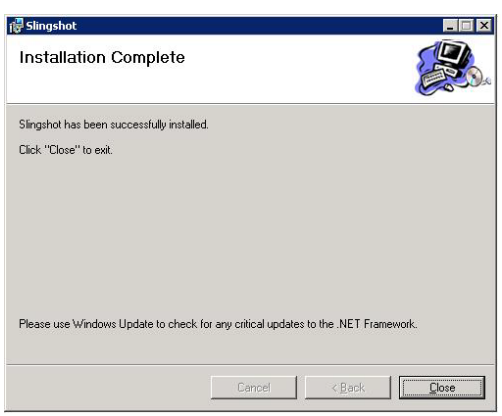

Figure 20

The plug-in is now installed. For more information on how to use the Outlook Plug-in please see the *Slingshotv1.9.2 User Guide*.

▲ Back to Top

Defining a MFT Platform Server

Slingshot Browser Interface, Outlook Plug-in, and the Vault Server all house their files on the *LOCAL (generally the web server) server by default. If you have other Windows or UNIX MFT servers you would like to designate these jobs to, you can define server definitions for them in Slingshot. For this guide we are configuring the bare minimum needed for a MFT Platform Server. For more information on creating and managing server definitions please see *Slingshot v1.9.2 Administrator Guide*.

Navigate to **Servers > Add Server**

1) Type in a Server Name (any name).
2) Enter the MFT Platform Server IP address.
3) Enter in the IP Port the MFT Platform Server is listening on.
4) Server Type should be Platform Server.
5) Enter the server Platform. (Note: Use a Windows or UNIX MFT Platform Server for Slingshot)
6) Expand the section called *Server Credentials* (See Figure 24)
7) Enter in a default user, password, and a domain if needed.
8) Click the Add button.

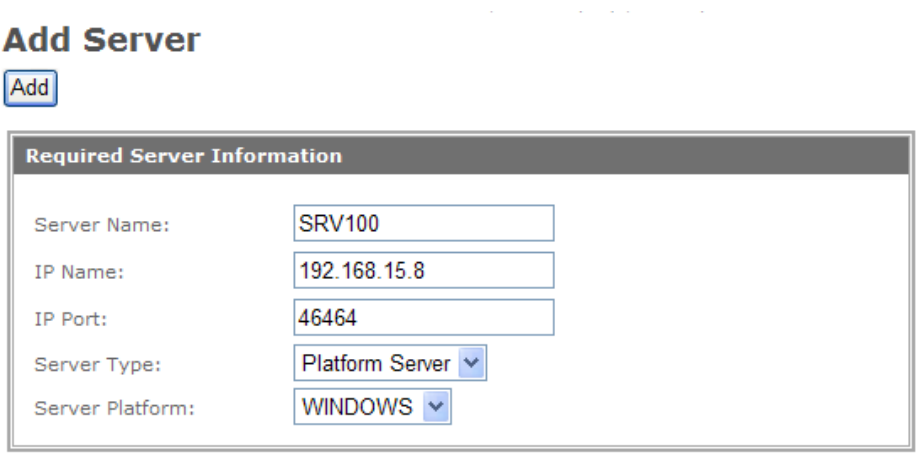

Figure 20

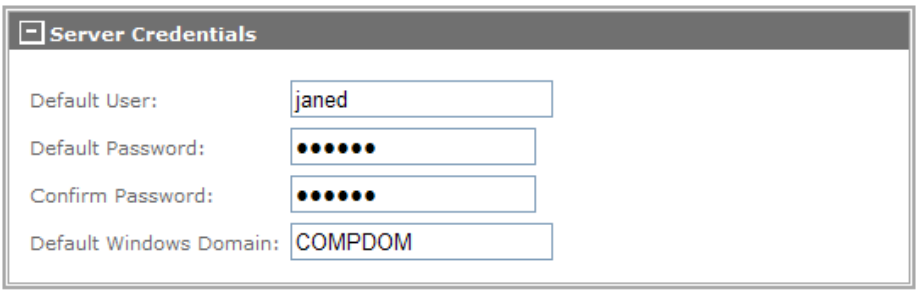

Figure 21

Your MFT Platform Server has been configured.

To further configure your MFT Platform Server to use PGP, read section Using PGP with Slingshot.

▲Back to Top

Slingshot Reports

Slingshot creates reports on all email file attachments uploaded and downloaded to the repository and Vault Server.

From the main menu navigate to **Reports > Attachments**

If you have sent any emails using Slingshot you will see here a summary of your email attachments and their current status.

Clicking on the *Subject* link for any message will provide more detailed information regarding the transfer, including the file size, expiration date and archive date.

If you have many file attachments and would like to define your output expand the *Selection Criteria* box (See Figure 25) and fill in one or more of the fields available and click on the Search button.

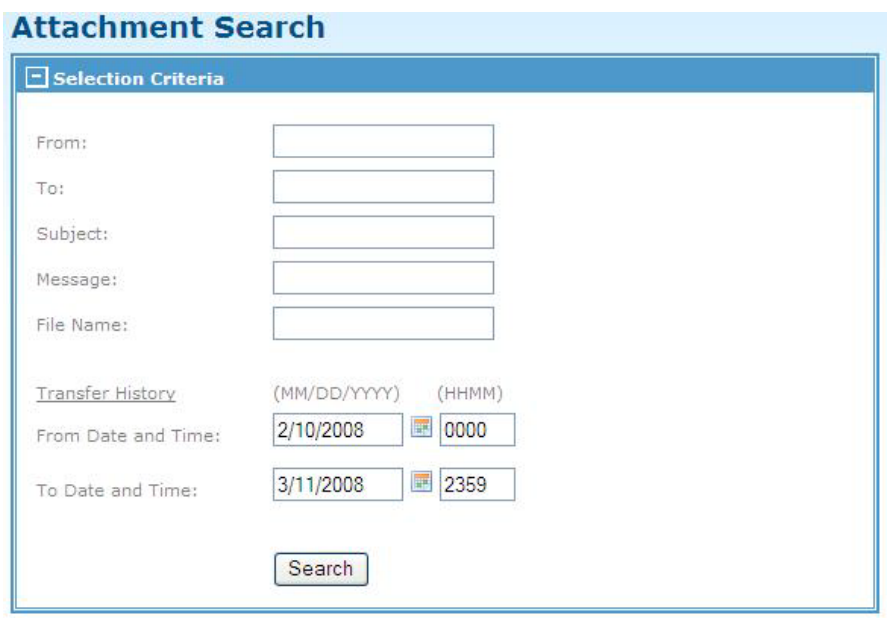

Figure 22

▲Back to Top

Using PGP with Slingshot

PGP Encryption can be used with Slingshot to increase data security. What this will do is allow files to be encrypted when they are uploaded to the repository by a sender and decrypted while being downloaded by the recipient. This is also the case when archiving files.

Step 1: Create a PGP System Key

When you want to have a file encrypted while it is being uploaded to the Slingshot repository you must configure a server to be a PGP server.

First Navigate to **Management > Keys > PGP System Key > Create**. Fill in the required information represented by the red * asterisk and then click on the Create Key button. Note: You can have more than one PGP System Key but only one can be the Default key. See example below:

Figure 23

Step 2: Add a PGP Server

Now navigate to Servers > Add Server. Fill in the Required Server Information section and then expand the PGP Information section. Here you will Enable PGP. By checking off this box ALL files going to this server will be PGP encrypted on an upload using the default PGP Server Key we created in Step 1. You can set more options in this section but for our example we are using the minimum settings.

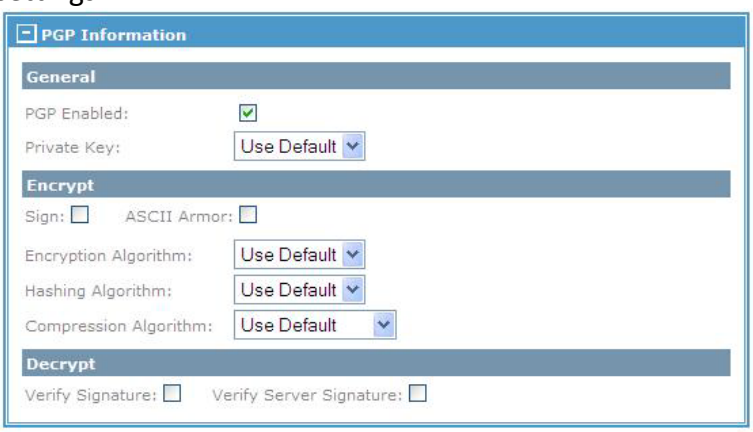

Figure 24

Step 3: Assign the PGP Server a PGP Public Key to use

Now we have to set e PGP Public key to be used when a file is downloaded from the repository by a recipient. To assign a PGP Public Key to the PGP Server that you defined in Step 1 we must first copy the PGP Public Key created when we created the PGP System Key.

Navigate to **Management > Keys > PGP System Keys > Manage PGP Keys**.

1) Click on the Description of the key you created in Step 1.
2) Expand the PGP Public Key section.
3) Copy the entire public key information in the text box.
4) Navigate to **Management > Keys > PGP Public Keys > Add PGP Key**
5) Select **Server**.

6) Choose the Server from the drop down list you created in Step 1.
7) Select **Enabled**.
8) Paste the PGP Public Key you copied in the step above.

Figure 25

Step 4: Configure the new MFT Platform Server in Slingshot Configurations

Now you would define the new PGP Server in your Slingshot Configurations web page. You can do this for both the Repository and/or the Vault Server

Navigate to **Management > Slingshot > Configurations**

9) Click the drop down menu and select the server you created in Step 1.
10) Edit the repository path if needed.
11) Click the Update button.

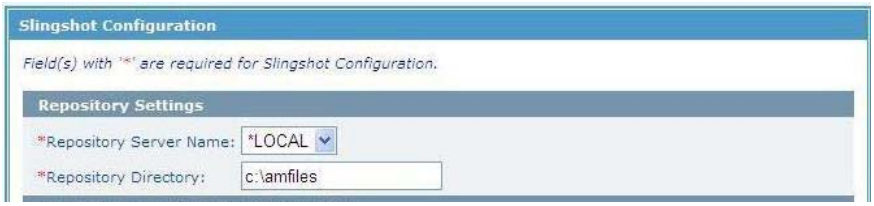

Figure 26

Now file attachments being sent via Slingshot Browser or Outlook Plug-in will be PGP encrypted and decrypted on a file upload and download.

▲Back to Top

More on Slingshot Assigned Rights

The only right needed for a Slingshot User to be able to download and upload files using the Slingshot Web Browser Interface or Outlook Plug-in is the **TransferRight**.

Depending on the Slingshot configurations defined in Slingshot a new Slingshot User created will only be able to send an email with an attachment to any other Slingshot User in the Slingshot database or won't be able to send anything and simply be a recipient. We discussed configuring Slingshot's configurations in section 3.

There are specific rights for Slingshot Users to manage Users, Reports and Slingshot's configurations. They are as follows:

- **UpdateAttachmentRight** – This will allow a user to edit the configurations in the Slingshot configurations under **Management > Slingshot > Configurations**.
- **ViewAttachmentRight** – This right will allow a user to go into the **Reports > Attachments** web page and see the attachments. They will have the ability to Disable/Enable attachments. To be able to view the email content that was sent with the attachments see ViewEmailContentsRight.

Note: A Slingshot user with the AdministratorRight by default does not need the 2 above rights.

- **ViewEmailContentsRight** – This will allow the Slingshot/Slingshot user to be able to view the email contents of the attachments in the **Reports > Attachments** section.

By default, the ability to assign a Slingshot/Slingshot user the ViewEmailContentsRight is granted to Admin. Only he has the ability to assign another user this capability. If you want to assign another user this capability you must edit the cfcc web.xml file.

Open the web.xml for editing in notepad. Do a find for, ViewEmailContentsRight. You will see:

```
<context-param>
    <param-name>AssignViewEmailContentsRight</param-name>
    <param-value>admin</param-value>
</context-param>
```

This parameter is comma delimited. To add a user id, insert a comma after Admin and type in the new user id. See below:

```
<context-param>
    <param-name>AssignViewEmailContentsRight</param-name>
    <param-value>admin,JRJones</param-
value>
</context-param>
```

After making this change or any change, to the web.xml file you must restart your web server for the change to take place.

To modify a user's information, login to Slingshot and navigate to **Users > Manage Users**. Make any change necessary and click on the *Update* button. *(For more information on managing user accounts in Slingshot and the other rights available see Slingshot v1.9.2 Administrator Guide.)*

▲Back to Top

Disable Slingshot Outlook Plug-in

If for any reason you need to use Outlook without the Slingshot Outlook Plug-in. A local Administrator can Disable Slingshot by closing the Outlook window if it is open and navigating to:

Start > Programs > Slingshot > Slingshot Utilities

Figure 27

Simply click on the Disable button and Slingshot will no longer effect Outlook. At this point the Disable button will change to read Enable for you to enable Slingshot again when needed.

▲Back to Top