TIBCO Slingshot

Administrator 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.

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.

Contents

Preface

This manual provides instructions for using Slingshot. The manual guides you through the configuration of Slingshot and all of its components. Consult your network manager regarding network equipment and procedures at your installation site.

This publication is intended for those ***individuals*** responsible for configuring and operating Slingshot

Topics

Related Documentation

This section lists documentation you may find useful.

TIBCO Slingshot Documentation

The following documents form the TIBCO Slingshot documentation which can be viewed and downloaded from https://docs.tibco.com/products/tibco-slingshot-1-9-4:

- *TIBCO Slingshot Release Notes* Read the release notes for a list of new and changed features. This document also contains lists of known issues and closed issues for this release.
- *TIBCO Slingshot Installation Guide* Read this manual for instructions on site preparation and installation.
- *TIBCO Slingshot Administrator Guide* Read this manual for instructions on configuring the Slingshot Server after the installation.
- *TIBCO Slingshot User Guide* Read this manual for instructions on using the product to perform file transfer requests and more with Slingshot browser and Outlook Plug-in interfaces.

How to Contact TIBCO Customer Support

For comments or problems with this manual or the software it addresses, contact TIBCO Support, as follows:

- For an overview of the TIBCO Support and information on getting started with TIBCO Support, visit http://www.tibco.com/services/support
- If you already have a valid maintenance or support contract, visit https://support.tibco.com

  Entry to this site requires a user name and password. If you do not have login credentials, click Register with Support.
- Technical Support email address support@tibco.com
- Technical Support Call Centers:
  - North and South America: +1.650.846.5724 or +1.877.724.8227 (1.877.724.TACS)
  - EMEA (Europe, Middle East, Africa): +44 (0) 870.909.3893
  - Australia: +61.2.4379.9318 or 1.800.184.226
  - Asia: +61 2 4379 9318

Login

This section explains how to login to the Slingshot Administrator once the product has been installed.

Topics

- *Administrator Login*

Administrator Login

Once Slingshot is installed and configured, it is time to access the Slingshot Administrator web page. To login use the following URL substituting the areas of the URL with your install configurations:

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

Application Server	Default Port
Embedded Web Server	443

Enter Username: “admin”
Password: “changeit” (case-sensitive)

Figure 1

Users

The Users section defines and manages Users and Departments.

Topics

- *Add User*
- *Manage Users*
- *Departments*

Add User

You must add users to the Slingshot database in order for people to send emails with and attachments through Slingshot. There are several methods to add users to the Slingshot database. One is to directly add them through the Slingshot Administrator Add User web page by simply filling in the necessary and optional fields and click on the Add button. Another way is to add users through an LDAP server (Microsoft Active Directory), see section 6 for more information. A third method, which you can read more about in the *Slingshot Users Quick Start Guide*, is for an existing Slingshot user to send an email with a file attachment via the Slingshot Outlook Plug-in or the Slingshot Browser Interface to a new user. We will be discussing method one below.

First, you must be a Slingshot Administrator in order to add users through the Add User web page. This means your user id must have either of the following assigned right AdminstratorRight or UpdateTransferUserRight. To read more about administrator accounts please see the Assigned Rights parameter description below.

Navigation: Users > Add User

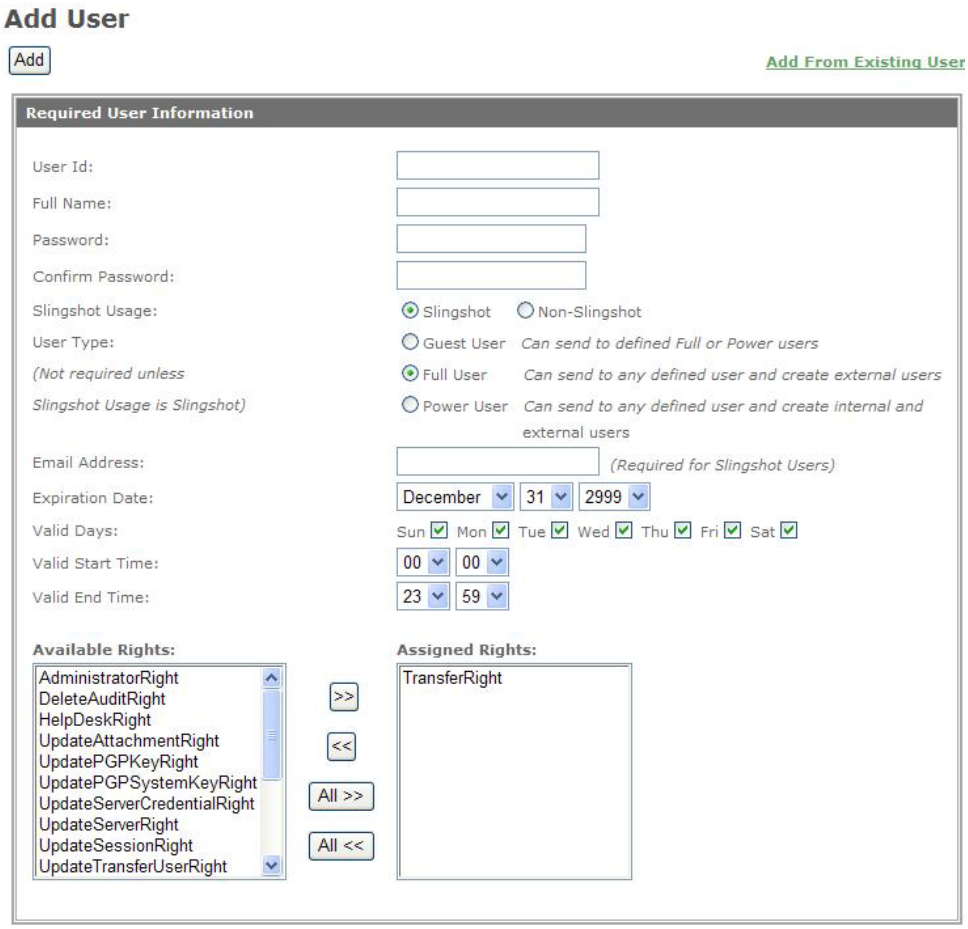


Figure 2

Figure 2 above shows the required fields needed to be set for a new user. Some of required information for a users account have been preconfigured for instance the users account will not expire until Dec. 31, 2999.

Required User Information - In the table below we will discuss each parameter to be set for a user in this window:

Parameter	Description
User Id	The Id the user will use to login to the different Slingshot Interfaces. Note: This will be a user's email address if a user is created via sending an

Parameter	Description
	email with an attachment for the first time.
Full Name	The user's full name (For instance First and Last name)
Password	Password for the user to type in when he/she logs in to the product.
Confirm Password	Password for the user to type in when he/she logs in to the product.
Slingshot Usage	By default a user will be set to be a Slingshot user with the assigned right of TransferRight so he/she can send emails with attachments via Slingshot. By setting the user to be Non-Slingshot, you must remove the TransferRight that is assigned and they will not be able to send emails with attachments via the Slingshot product. (These users are generally used for Slingshot administration purposes.)
User Type	The three types of Slingshot users that are available at this time are as follows: Guest User - External users who have the right to send or receive files to any Full user or Power user but cannot send to other guest users. Guests can not view the Contacts list. They can only send to Full and Power users they know email addresses for. Full User - Internal users with the right to send and receive emails to anyone outside the organization or to any other internal user. A Full user has the ability to add new Guest users via email. Power User - Internal users with all the rights of a Full user. In addition, a Power user is able to automatically add new Full users via email.
Email Address	The user's email address that Slingshot will use to send emails with file attachments.
Expiration Date	The date the user's account will expire.
Valid Days	The days the user will be allowed to login to the Slingshot Interfaces.
Valid Start Time	The time of the day the user will be allowed to login to the Slingshot Interfaces. This value coincides with the Valid Days the user can login.

Parameter	Description
Valid End Time	The time at which the user will no longer be allowed to login to the Slingshot Interfaces. This value coincides with the Valid Days and Valid Start Time the user can login.
Assigned Rights	By default a user is assigned the TransferRight which is all that is needed for them to send emails with file attachments via Slingshot. However, we provide many rights to allow a single user to be assigned additional Slingshot administrative responsibilities. By assigning a user any other right than the TransferRight you will be giving them the ability to login to the Slingshot Administrator web pages and to perform the duties given to them by the assigned right. For descriptions for all the available rights please see the Available Rights table. Warning: By assigning any user the AdministratorRight you are turning that user account into a Super administrator account. By default the pre-existing user accounts 'admin' and 'SSAdmin' are both super administrator accounts. Note: by assigning a user the AdministratorRight and placing them into a Department you are creating what we refer to as a Delegated Administrator which is a user that can only perform administrator functions over the users within that same department. He/she cannot change any Slingshot system configurations.

The **Add From Existing Users** link will work if you have a predefined user account that you want to copy all the properties of, like a template user account. The link will open the Manage Users web page which displays your existing user accounts. Once you have clicked on one of them out of the list Slingshot will import all the values of the existing user into the Add User web page and allow you to supply the User Id, Full Name, Password, and Email Address.

Available Rights

Right	Description	Description using Delegated Administration
AdministratorRight	Allows a user to perform all administrative functions within the Slingshot system. This right does not include TransferRight or any function that corresponds to this right.	Allows a user to perform all administrative functions within their Department. This right does not include TransferRight or FTTransferRight or any functions that correspond to these rights. The Department Administrator cannot update Server or Server Credentials unless given UpdateServerRight and UpdateServerCredentialRight.
DeleteAuditRight	Allows any user to delete Audit Record.	Allows any user to delete Audit Record. Department checking will not be done.
HelpDeskRight	Allows a user to change another user's password, turn on and off the disable flag for a user as well as turn on and off the lock flag for a user.	Allows a user to change another user's password, turn on and off the disable flag for a user as well as turn on and off the lock flag for a user.
TransferRight	Allows a user to execute Slingshot transfers.	Allows a user to execute Slingshot transfers.
UpdateAttachmentRight	Allows a user to edit the configurations in Management>Slingshot>Configuration web page.	Allows a user to edit the configurations in Management>Slingshot>Configuration web page.

Right	Description	Description using Delegated Administration
UpdatePGPKeyRight	Allows a user to add and manage the configurations of Slingshot's PGP Public Key's contained in Management>Keys>PGP Public Keys>Add or Manage PGP Keys.	Allows a user to add and manage the configurations of Slingshot's PGP Public Key's contained in Management>Keys>PGP Public Keys>Add or Manage PGP Keys.
UpdatePGPSystemKeyRight	Allows a user to add and manage the configurations of Slingshot's PGP System Key's contained in Management>Keys>PGP System Keys>Add or Manage PGP Keys.	Allows a user to add and manage the configurations of Slingshot's PGP System Key's contained in Management>Keys>PGP System Keys>Add or Manage PGP Keys.
UpdateServerCredentialRight	Allows a user to view or update Server Credential configured for a Server.	Allows a user to view or update Server Credential configured for a Server.
UpdateServerRight	Allows a user to view or update Slingshot Server records.	Allows a user to view or update Slingshot Server records in their own Department. New Servers cannot be added.
UpdateSessionRight	Allows a user to view and delete active user sessions.	Allows a user to view and delete active user sessions.

Right	Description	Description using Delegated Administration
UpdateTransferUserRight	Allows a user to view and update Slingshot User records. Only TransferRight can be given to a user unless you are an administrator. The Super Administrator can assign any right to a user.	Allows a user to view and update Slingshot User records. Only TransferRight can be given to a user unless you are an administrator. The Department Administrator can assign any rights to a user within their Department except UpdateServerRight and UpdateServerCredentialRight.
ViewAttachmentRight	Allows a user to view the attachment requests listed in Reports>Attachment.	Allows a user to view the attachment requests listed in Reports>Attachment.
ViewAuditRight	Allows a user to view Audit records.	Allows a user to view Audit records.
ViewEmailContentsRight	Allows a user to view the emails contained in the attachment requests listed in Reports>Attachment. (This right would accompany ViewAttachmentRight or AdministratorRight)	Allows a user to view the emails contained in the attachment requests listed in Reports>Attachment.
ViewGroupRight	Allows a user to view Group records.	Allows a user to view Group records.
ViewPGPKeyRight	Allows a user to view PGP Public Keys contained in Management>Keys>PGP Public Keys>Manage Public Keys.	Allows a user to view PGP Public Keys contained in Management>Keys>PGP Public Keys> Manage Public Keys.

Right	Description	Description using Delegated Administration
ViewServerCredentialRight	Allows a user to view Server Credentials configured.	Allows a user to view Server Credentials configured.
ViewServerRight	Allows a user to view Servers configured.	Allows a user to view Servers configured.
ViewSessionRight	Allows a user to view active user sessions.	Allows a user to view active user sessions.
ViewUserRight	Allows a user to view Users configured and the Rights associated with those users.	Allows a user to view Users configured and the Rights associated with those users.

Optional User Properties

In Figure 3 below you will see the optional parameters that can be set for a user after you expand this window:

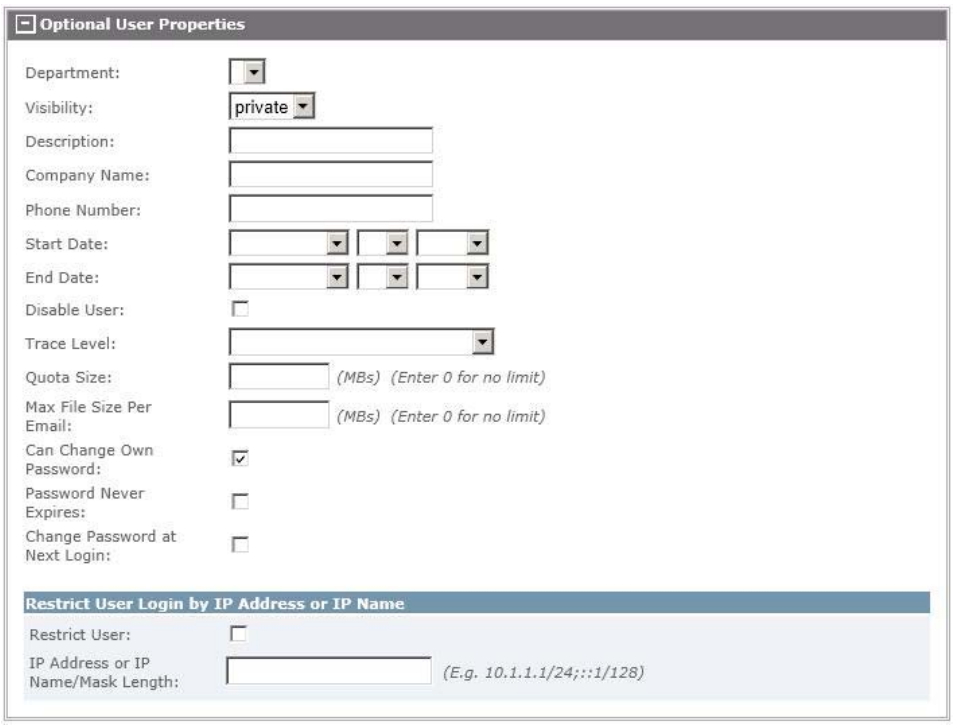


Figure 3

Each optional parameter is discussed in the table below:

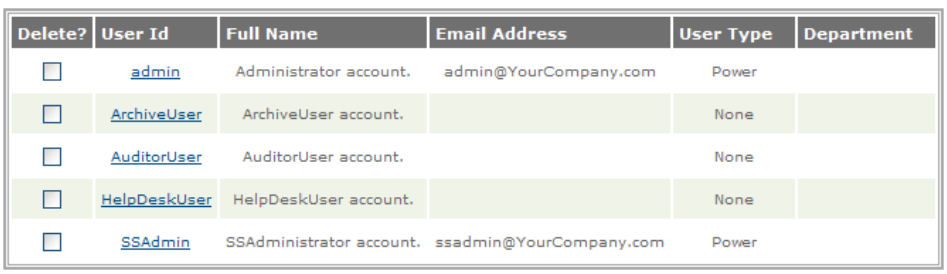
Parameter	Description
Department	The department you want to assign the user to. (For more information on Departments see the section Departments.) Warning: In a multi-server environment you need to create the same departments on each server.
Visibility	This parameter will come in affect when a user is assigned to a department. The “Visibility” allows departments to interact with each other without giving up administrative control. Public – Can be seen by all users in the system Private – Can only be seen by users in the same department

Parameter	Description
	When applied to Users or Servers, visibility allows Departments to expose or hide these items from each other. This is achieved by setting the visibility to public or private. For example, by default the Sales Department users with the visibility of private can send or receive emails to only user's within their department. However, if the Accounting Departments users are set with a visibility of "public" the Sales department users will also be able to send and receive to the Accounting Department. If an Accounting User has been set to "private", the Sales Department can not send or received an email to that user. In this case the user is effectively hidden from other Department. If a Sales Department user contains the AdministratorRight that user can only manage the users in the department he is a member of. He will not be able to make any changes to the Accounting Department users in spite of their visibility being set to public. *Warning: Changing an administrator's department will remove their super administrator rights.* All users not assigned to a department are visible to all users whether they are in a department or not.
Description	An alpha numeric field available to enter a description for this user.
Company Name	An alpha numeric field available to enter a company name for the user.
Phone Number	An alpha numeric field available to hold a users telephone number
Start Date	The date in which the users account can be used to login to the Slingshot Interfaces.
End Date	The date in which the user account can no longer login to the Slingshot Interfaces. (If the Expiration Date occurs prior to the End Date set this will take precedence over this field and vice versa. Whichever date comes first for these two fields will stand.
Disable User	This checkbox disable's a user's account preventing them from logging into the Slingshot Interfaces.
Trace Level	Sets the trace level to be used when this user is logged in using any of the Slingshot Interfaces. *Note: This should only be set when requested by TIBCO's Technical Support.*

Parameter	Description
Quota Size	Amount of disk storage space that can be used by the user for sending attachments. Unless a value is entered into this field, a user's quota limit will be controlled by the global quota size set on the Slingshot Configuration page.
Max File Size Per Email	Maximum size of a file that can be sent by a user in a single email. Unless a value is entered into this field, a user's file size limit will be controlled by the global file size limit set on the Slingshot Configuration page.
Can Change Own Password	This checkbox allows a user to change their password.
Password Never Expires	This checkbox sets the user's password to never expire.
Change Password at Next Login	This checkbox forces the user to change their password the next time they login. *Note: If a Slingshot administrator changes the users password in the Update User web page this checkbox will automatically be enabled.*
Restrict User	This checkbox will restrict a user to only be able to login to the Slingshot Interfaces when connecting with a specific IP or IP Name and/or Netmask.
IP Address or IP Name/Mask Length	IP Address or IP Name this user must be using when he/she is logging into any of the Slingshot Interfaces.

Manage Users

To manage your user accounts you would navigate to the Users > Manage User web page. In Figure 4 below you will see the pre-existing user accounts that exist after Slingshot has been installed:



Delete?	User Id	Full Name	Email Address	User Type	Department
☐	admin	Administrator account.	admin@YourCompany.com	Power	
☐	ArchiveUser	ArchiveUser account.		None	
☐	AuditorUser	AuditorUser account.		None	
☐	HelpDeskUser	HelpDeskUser account.		None	
☐	SSAdmin	SSAdministrator account.	ssadmin@YourCompany.com	Power	

Figure 4

For users who authenticate against LDAP you will not be able to edit the following fields:

- Full Name
- Primary Email Address
- Telephone Number

Any other fields you may edit and they will NOT be changed as a result of an LDAP Sync taking place.

Warning: When editing a user's account in a multi-server or multi-database environment you will need to edit that user's account for each instance.

The Manage Users web page will display 100 defined users at a time. If there are more than 100 users defined, you would click on List Next 100 > to access the next 100 user definitions. Use the Back button to see the previous definitions.

A brief description of the pre-existing user accounts and what they are used for is below:

Template User ID	Description
ArchiveUser	ArchiveUser is needed for the following purposes: : Allows you to set Server Credential for this account when sending data to a MFT Platform Server : Set Trace settings for Vault Server : Picks up the email address for Archive Status emails. *Warning: If the 'ArchiveUser' is deleted, the Vault Server utility will not function. You would have to recreate the user account to restore the functionality.*
AuditorUser	An example audit user's account.
HelpDeskUser	An example Help Desk User's account.
SSAdmin	A Super Administrator account.
admin	A Super Administrator account.

Delete a User Account

To delete a user, select the check box next to the user that you wish to delete and click on the Delete button at the bottom of the screen. Multiple users may be deleted at one time.

Search for a Specific User Account

You can search for a particular user(s) by entering information in the Selection Criteria window for any combination using the fields shown below:

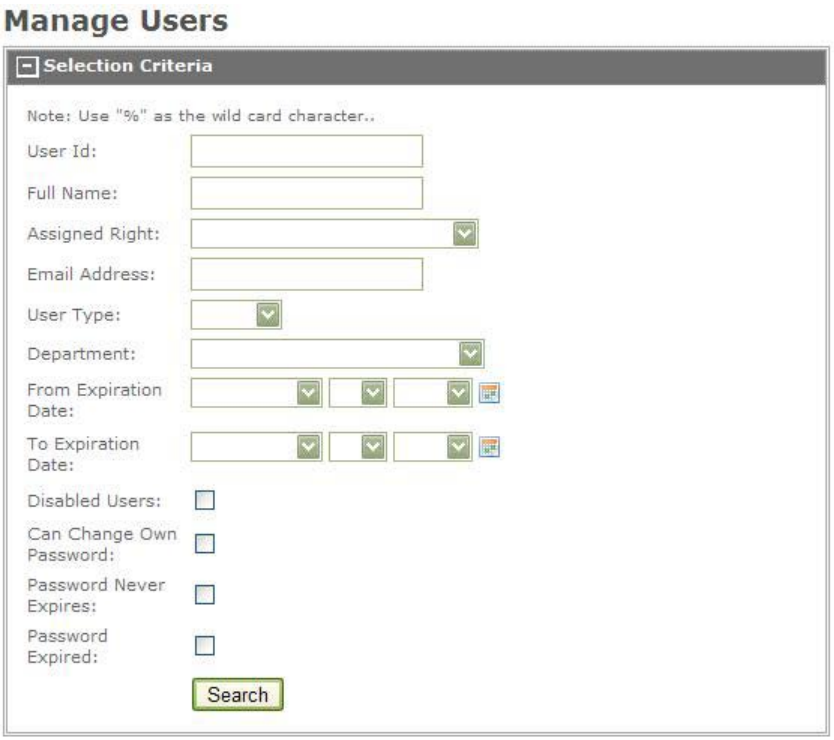


Figure 5

The % character is used as a wildcard character to simplify the search. For instance to search for the user johnsmith you could enter “johns%” in the User Id field.

Update a User Account

To update a user, click on the User Id of the user that you would like to change. Once the changes are made, click on the Update button to save the changes.

The parameters and fields are the same on the Update User web page as on the Add User web page. As such please refer to the Add User section of this manual for the parameters and their descriptions.

Warning: If you change an administrator's department you will remove their super administrator rights.

Departments

Users who are not assigned to a department will be able to view every contact in the address book as well as send attachments to all users on the system. If this is something you do not want, then you would assign users to Departments. Departments provide the ability to segregate users so that they may not view or send email attachments to users in other departments.

Warning: In a multi-server environment you need to create the same departments on each server.

Add a Department

Only a super administrator can add departments to Slingshot.

Navigate to: Users > Departments > Add Department

Figure 6

Once you have filled in the Required Department Information click the Add button.

Manage Departments

Navigation: Users > Departments > Manage Departments

Figure 7

Delete a Department

To delete a Department definition, select the check box next to the Department you want to delete and click on the Delete button. Multiple Department definitions may be deleted at one time.

Update a Department Description

To update a departments Description you would click on the Department Name that you would like to edit the description for. Make the changes you require and click on the Update button.

Servers

By default file attachments that are emailed with the Slingshot products are stored in a local repository and archived locally on the system where Slingshot is installed. Depending on the volume of users sending files with Slingshot and the size of those files storage on the web server may become an issue.

To have your repository and/or archived files located on a Windows or UNIX machine you would use the Add Server web page to define a MFT Platform Server to house those files. You can user either a MFT Platform Server installed on a UNIX or Windows platform to store your files. If you do not presently have a MFT Platform Server installed contact a TIBCO representative at support@tibco.com.

Warning: If you are using a MFT Platform Server for your repository and/or Vault server it is not recommended changing the Server definition once it is configured. For example setting PGP keys for the MFT Platform Server where they were not used in the past.

Topics

Add Server

Navigation: Servers > Add Server

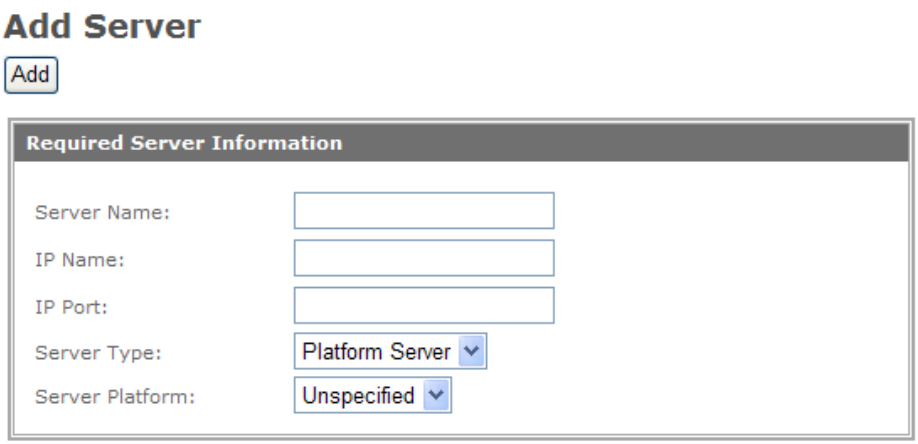


Figure 8

Figure 8 above shows the required fields needed to be set for a new MFT Platform Server.

Required Server Information

In the table below we will discuss each parameter to be set for a server in this window:

Parameter	Description
Server Name	Defines the name to be used to represent the MFT Platform Server.
IP Name	The IP or host name for the MFT Platform Server.
IP Port	The port this MFT Platform Server is listening on. (Generally it is 46464)
Server Type	Defines this server as a Platform Server or the LOCAL server.
Server Platform	Define whether this MFT Platform Server server is a Windows or UNIX server.

Slingshot Options

The Slingshot Options allows you to define the **Default Encryption Type** to be used between the Slingshot Administrator and the MFT Platform Server. Be careful when encrypting data because of the CPU overhead that is required. If your application requires encryption, we suggest using AES(Rijndael) encryption because it is more secure and more efficient than DES encryption.

Local Options

The Local Options allows you to define the **Server File Name Prefix** which is used when the Server Type is defined as LOCAL. It is a directory name that will be prefixed to the Server File Name that is defined on a transfer record. This allows you to restrict users to access particular directories.

Server Credentials

The Server Credentials are ignored for Servers defined with Server Type of LOCAL but when working with a MFT Platform Server it is necessary to define a user's credentials to allow Slingshot to login to the MFT Platform Server to read and write files. This user's credentials will be used for all files being sent and received by this server regardless of the Slingshot user sending and receiving files:

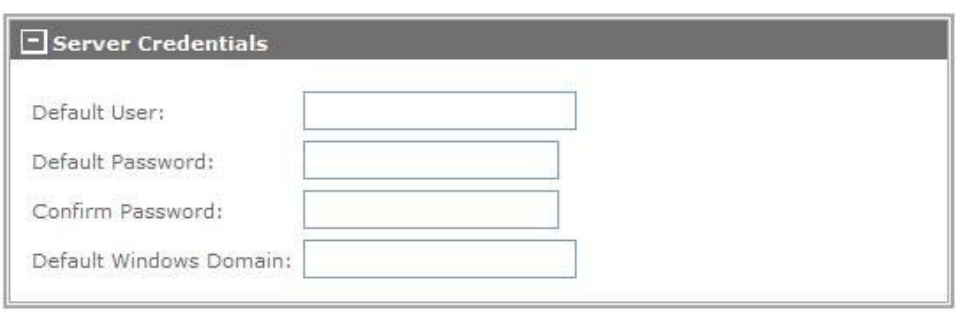


Figure 9

In the table below we will discuss each **Server Credentials** parameter seen in figure 9 above:

Parameter	Description
Default User	Windows or UNIX user id to use for logging on to the system.

Default Password	The default user's password. A password containing any of the characters below cannot be used to authenticate to a Windows computer: ^, [,]
Confirm Password	Enter the default user's password a second time to confirm it.
Default Windows Domain	If the MFT Platform Server is on a Windows machine, what is the domain name for the user's account?

Additional Server Properties

Each server has additional server properties that can be set for it. Figure 10 shows the Additional Server Properties window expanded for you to see.

Figure 10

In the table below we will discuss each parameter that can be set for the **Additional Server Properties** window:

Parameter	Description
Department	Drop down list of the departments available to place this server in. If there is nothing to choose from then there are no departments created.
Visibility	This parameter will come in affect when a user is assigned to a department. The "Visibility" allows departments to interact with each other without giving up administrative control. Public – Can be seen by all users in the system Private – Can only be seen by users in the same

Parameter	Description
	department When applied to Users or Servers, visibility allows Departments to expose or hide these items from each other. This is achieved by setting the visibility to public or private. For example, by default the Sales Department users with the visibility of private can send emails to only user's within their department. However, if the Accounting Departments users are set with a visibility of "public" the Sales department users will also be able to send to the Accounting Department. The administrative control of the emails will still belong to the Sales Department that sent them but the ability to send emails is given to the users in the Accounting Department. The Sales Department can in no way alter the attributes of the users from the Accounting Department. If an Accounting User has been set to "private", the Sales Department can not send an email to that user. In this case the user is effectively "hidden" from other Department.
Disable Flag	Enable this box if you want to disable this server.
Description	Alpha numeric field to hold a description for this server.
Trace Level	Sets the trace level to be used when this server is being used by any of the Slingshot Interfaces. *Note: This should only be set when requested by TIBCO's Technical Support.*

PGP Information

You can associate a PGP key to be used with a MFT Platform Server. Figure 11 shows the PGP Information that can be configured. What this means is all data sent to or received from this server will use PGP encryption/decryption. Note that PGP Encryption is performed on an Upload (i.e. Writing data to the MFT Platform Server) while PGP Decryption is performed on a Download (Reading data from a MFT Platform Server). That means that data written to a Server with PGP enabled will be PGP encrypted and then written. Data read from a Server with PGP enabled will be read and then PGP decrypted.
Note: Due to the way PGP Compresses and Encrypts data, Checkpoint Restart is not supported for PGP Transfers. If Checkpoint Restart is turned on for a PGP transfer, it will be ignored.

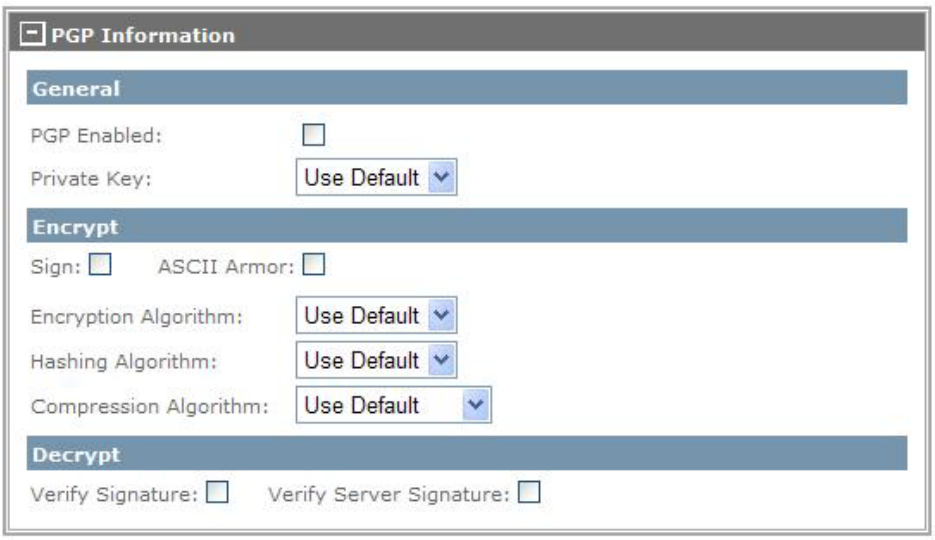


Figure 11

In the table below we will discuss each ***parameter*** that can be set for the **PGP Information** window:

Parameter	Description
PGP Enabled	Enables PGP processing on all files being sent and received from this server.
Private Key	The PGP Private Key that will be used when Decrypting or Signing data. The dropdown list will contain any PGP Private keys that have been added to the system or you can use the default PGP.
Encrypt: Sign	Defines whether MFT Platform Server will sign the PGP encrypted data. Note: The end user will require the corresponding PGP Public Key to validate the signature.
ASCII Armor	Defines whether MFT Platform Server will convert the data to PGP ASCII Armored format. ASCII Armored format is a Base64 conversion that allows binary data to be represented in a character format. This option should be left off unless there is a specific reason to use it.
Encryption Algorithm	Allows the user to define the Encryption Algorithm that will be used for PGP Encryption. In most cases it is best to use the default value.
Hashing Algorithm	Allows the user to define the Hashing Algorithm that will be used for PGP Encryption. In most cases it is best to use the default value. Note: Bouncy Castle only supports

Parameter	Description
	signatures using a DSA signing key with hashing algorithm SHA. If are using an RSA signing key any of the hashing algorithms can be used.
Compression Algorithm	Allows the user to define the Compression Algorithm that will be used for PGP Encryption. In most cases it is best to use the default value.
Decrypt: Verify Signature	Defines whether we will verify the signature of incoming data. If this box is enabled, and the data is not signed or signed incorrectly, the request will fail.
Decrypt: Verify Server Signature	Adds an extra layer of Signature protection. When the signature is verified, this parameter insures that the signature was validated with the PGP Public Key associated with this Server definition. Otherwise, the signature will be validated against PGP keys associated with any user or server.

Manage Servers

Navigation: Servers > Manage Servers

The Manage Servers page allows you to list and update any Slingshot Server definitions. Server Definitions define the settings necessary for Slingshot to access the MFT Platform Server systems where the repository or archived files are located.

Selection Criteria

This box allows you to selectively search the Server record database to limit the number of records that are displayed in the Results table. The % character is used as a wildcard character to simplify the search. If a field has no search criteria entered, then no filtering will be done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a record will be returned. When you have completed the Search Criteria, click on the Search button. The output will be placed in the Results table. Up to 100 Server definitions will be displayed at a time within the Results table. If more than 100 entries are returned for a search, you can view the next 100 entries by clicking on List Next 100>. If you click on the Server Name of an entry in this table, a detail page will be displayed that allows you to update the server configuration if you are authorized.

Management

Under Management you can set Global Password Rules, configure Slingshot settings, view active sessions, and add users with an LDAP server.

Topics

- *System Configuration*
- *Slingshot*
- *Alerts*
- *Keys*
- *Activity*
- *Authenticators*
- *LDAP*
- *Lockout*

System Configuration

The System Configuration page allows you to set default Global Password Rules for the Slingshot Users and view the Local Settings for the Slingshot server.

Global Password and Self Registration Rules

In this section the Administrator can configure Global rules for changing and expiring passwords.

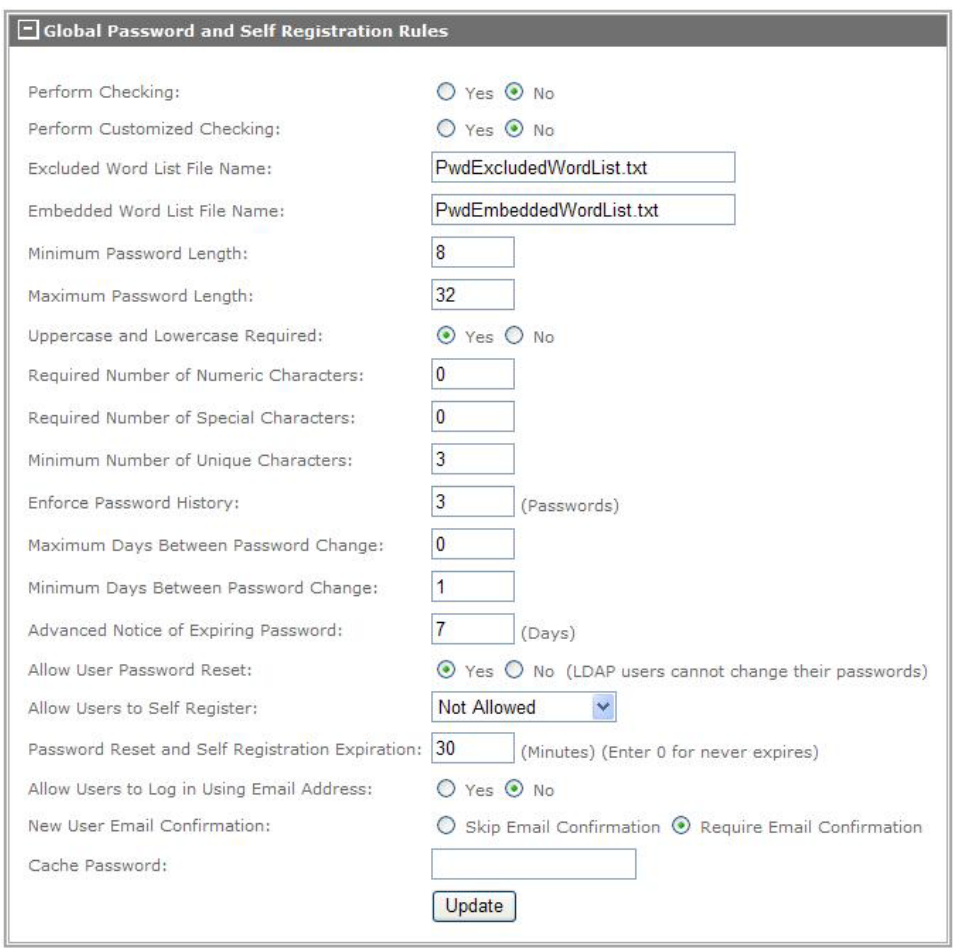


Figure 12

Parameter	Description (Underlined values are default)
Perform Checking	Will password rules will be enforced. Valid values: Yes or No
Perform Customized Checking	Did you create your own customized java class to check your own specific rules you want user's to follow? Valid values: Yes or No Customized rules allow you to write your own JAVA code to enforce password rules. Refer to the Slingshot documentation for more information on how to write a customized rule checking routine.
Excluded Word List File Name	The file name of the excluded word list, "PwdExcludedWordList.txt". It is located in (WEB_HOME)/webapps/cfcc/pwdconfig directory. Words in the Excluded Word List will be compared to a users the new password to see if there is an exact match (case insensitive). You may replace the file with another but it must be placed in the above directory. If the parameter is left blank no check will be done. Note: If you change the file, the change must be performed on each system where Slingshot is running.
Embedded Word List File Name	The file name of the Embedded word list, "PwdEmbeddedWordList.txt". It is located in (WEB_HOME)/webapps/cfcc/pwdconfig directory. Words in the Embedded Word List cannot be in any part of a user's the new password (case insensitive). You may replace the file with another but it must be placed in the above directory. If the parameter is left blank no check will be done. Note: If you change the file, the change must be performed on each system where Slingshot is running.
Minimum Password Length	The minimum length a password can be. Valid values: 1 - 32. Default: 8
Maximum Password Length	The maximum length a password can be. Valid values: 1 - 32. Default: 8 *Note: This parameter must be greater than or equal to the Minimum Password Length.*
Uppercase and Lowercase required	Are upper and lower case characters required in a password? Valid values: Yes or No.
Required Number of Numeric Characters	The minimum number of numeric characters between 1 and 9 required in a password. Valid values: 0 – 9
Required Number of	The minimum number of special characters required in a password. Valid values: 0 - the minimum password

Parameter	Description (Underlined values are default)
Special Characters	length. *Note: Special characters allowed in a password are dependent on the Web Server type, and the environment where the web server and browser client run.*
Minimum Number of Unique Characters	The minimum number of unique characters required in a password. Valid values: 0 - the minimum password length. Default: 3
Enforce Password History	Defines the number of passwords that are kept in the password history and cannot be reused. Valid values: 0 – 12. Default: 3.
Maximum Days Between Password Changes	The maximum number of days after a password change is done before the password will expire and the user is required to enter a new password. Valid Values: 0 - 999. 0 means users passwords will never expire. *Note: This parameter is ignored when a user's account has Can Change Own Password disabled or Password Never Expires is enabled.*
Minimum Days Between Password Changes	The minimum number of days after a password change is done a user must wait before they can change their password again. Valid Values: 0 – the Maximum Days Between Password Changes. Default: 1.
Advance Notice of Expiring Passwords	The number of days before a password expires that a user will receive notification. Valid values: 1 – 15. Default: 7.
Allow User Password Reset	Do you want to allow the user to reset their own password without them needing to know there current password? Valid values: Yes or <u>No</u>
Allow Users to Self Register	Defines whether users can self register. The following options are available in the drop-down box: : Not Allowed: Users are not allowed to self register : Guest Users Only: Only Guest Users are allowed to self register : Full Users Only: Only Full Users are allowed to self register : Guest and Full: Both Guest and Full Users are allowed to self register *Note: Guest and Full User settings are determined based on the Slingshot Configuration "Internal Email Domains" setting* *Note: Allow User Password Reset must be set to*

Parameter	Description (Underlined values are default)
	'Yes' in order to activate self registration.
Password Reset and Self Registration Expiration	The number of minutes Slingshot will wait for a user password reset request and/or self registration request to expire. This parameter is valid only when "Allow User Password Reset" is set to "Yes". Valid value: 0 – 30. If the user attempts to reset their password or self register after the interval expires, the request will be rejected.
Allow Users to Login Using Email Address	When this setting is enabled a user can login to Slingshot using their email address as well as their user id. Note: If the same email address in defined multiple times in the database the user will not be able to login with the email address.
New User Email Confirmation	Defines whether an email confirmation is required for: : First time users to set their password : Users to Self Register themselves Note that a first time user means that the user is defined to Slingshot, but has never successfully logged onto Slingshot. Users that self register are users that are not defined to Slingshot, but want to register with Slingshot. The registration process will create a Slingshot account for that user. The default value of No indicates that when a first time user resets their password, Slingshot will send a confirmation email to that user. The user must click on the URL in that email to set reset their password. Likewise for a user to register themselves, Slingshot will send a confirmation email to that user. The user must click on the URL in that email to set register with Slingshot. When this value is set to Yes a first time user can reset their password directly without waiting for an email. Likewise users can register themselves directly without waiting for an email. Warning: By default, Slingshot will require new users to verify their email address. If email confirmation is turned off, individuals being added to Slingshot will no longer have to confirm their identity via email verification. The setting applies to new users created via email, and new users created via self registration. This feature was implemented as an ease of use

Parameter	Description (Underlined values are default)
	alternative for Slingshot new user creation. TIBCO recommends using email confirmations if a strict level of attachment security is required by your organization.
Cache Password	This defines the password that will be used when updating the cache on other Slingshot servers that share the database. If this parameter is not defined, a default password will be used when updating the cache. Note: The current user's user id logged in to the system making any changes to the configuration is used when connecting to the remote system.

Customizing Password Rules

Slingshot allows you to write your own custom password checking rules. By taking a java class you have written and deployed you can replace ours and configure the system to use it.

The java class you will need to create and will be replacing is named PasswdRulesCustom.java in the package com.proginet.sift.util. This class must have a static method named CheckRules that takes two String parameters. The first is the user id and the second is the new password. This method does not return anything. A java.rmi.RemoteException should be thrown if you wish to prevent a password change that does not meet your custom rules.

Below is the PasswdRulesCustom class that is deployed by default which does nothing at this time:

```
package com.proginet.sift.util;

import java.rmi.RemoteException;

public class PasswdRulesCustom
{
   public static void CheckRules(String uid, String newPwd) throws
   RemoteException
```

```
        {
            return;
        }
    }
```

You would compile the class with the following command:

```
javac PasswdRulesCustom.java
```

Once you have compiled the class you can deploy it by overwriting the existing class located in the (WEB_HOME)\cfcc\WEB-INF\classes\com\proginet\sift\util directory. You must restart the server after deploying the new class.

Now go to the System Configuration page in the Slingshot administrator. Expand the Global Password Rules section set “Perform Customized Checking” to Yes.

Local Settings

Slingshot can be installed on a single server as well as on multiple servers within a network using different servers for authentication purposes. For each instance of Slingshot installed using the same database you will see a Local Settings window shown. Figure 13 below is an example of a single server instance:

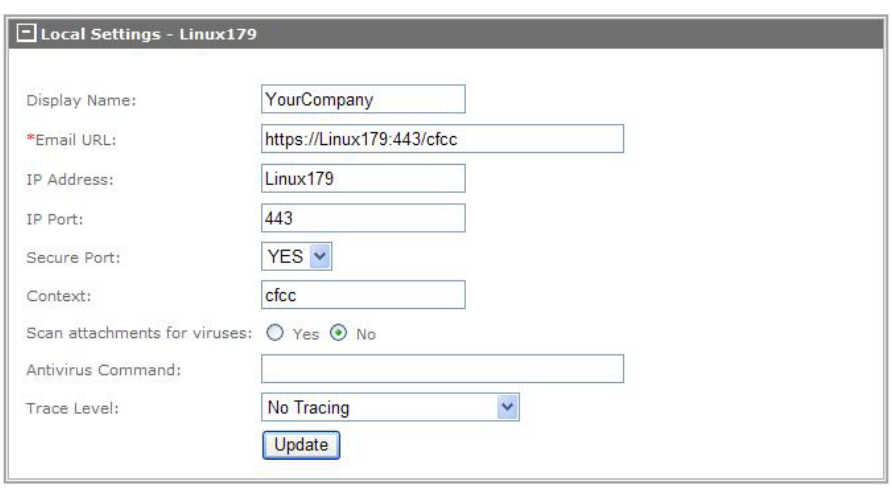


Figure 13

The **Display Name** field serves more than one purpose. First 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 13) and the Slingshot Web Browser Interface web pages (See Figure 14).

Figure 14

It is not recommend you change these fields unless absolutely necessary or advised by TIBCO's Technical Support team. A description for each field is in the table below for your convenience:

Parameter	Description (Underlined values are default)
Email URL	The URL that is being referenced in emails sent out by Slingshot. The URL typically points to the IP Name (DNS name) of the Slingshot server and is set during Step 4. Although you can use and IP Address it is not recommended because if a change to the IP address is ever needed in the future and emails with files attachments sent by users using the links to the Slingshot server in older emails will receive errors due to the file attachments not being able to be found.
IP Address	The IP Address of the Slingshot Server. This information is defined during the installation of the Slingshot server. It should only be updated when the IP Address changes.
IP Port	The IP Port of the Slingshot Server. This information is defined during the installation of the Slingshot server. It should only be updated when the IP Port changes.
Secure Port	Defines whether the IP Address and IP Port defined use HTTPS or HTTP protocol. If HTTPS is used, this box should be checked.

Parameter	Description (Underlined values are default)
Context	The context being used for this Slingshot instance. This information is defined during the installation of the Slingshot server.
Trace Level	Sets a Systemwide Trace Level for this Slingshot instance. We suggest leaving the Trace Level at "No Tracing" unless instructed by TIBCO Technical Support. Slingshot supports a variety of Tracing, so there may be a more efficient place to enable tracing than for the entire system.

Scan attachments for Viruses

Scan attachments for viruses defines whether Slingshot will call virus scanning software to check for viruses. Valid values are Yes and No. The default value of "No" means that virus checking will not be performed. The value "Yes" means that virus scanning will be performed. Note that if "Yes" is selected, the "Antivirus Command" parameter must be defined.

Antivirus Command defines the command that Slingshot will execute to check for viruses. This enables you to utilize your own virus scanning software within Slingshot. Slingshot interprets the return codes from the Antivirus command in the following manner:

0 means that no viruses were detected the attachments.

! = 0 means that a virus was detected in one of the attachments. Slingshot will disable the entire request.

The format for the Antivirus command depends on the virus scanning software being executed. The virus command can be executed directly or it can be executed as part of a script. There are a few important considerations when defining the Antivirus Command:

The fully qualified name of the virus program should be used

If there is a space in the script or program path, the fully qualified script/program path should be enclosed in double quotes

Use the token #(FileName) where the Antivirus script/program expects the file name. Slingshot will substitute the actual file name.

Make sure that the script returns a 0 for an attachment without a virus

Make sure that the script returns a non zero value for an attachment with a virus.

Here is an example command that would be entered into the “Antivirus Command” field:

“C:\Program Files\AntiVirus\bin\vscan" -remove=yes #(FileName)

Lockout Rules

Navigation: Management > System Configuration > Lockout Rules

For added security, the Slingshot server can automatically detect if a user is trying to repeatedly access an account with an invalid password or UserID. Once the configured number of failed login attempts has been reached, the Administrator has the option of locking the offending user and/or receiving an alert email. Users can be locked out by UserID or by IP address. Lockout rules are in effect for both the browser and the Outlook plugin login functions.
The system itself can be locked out after a configured number of failed global login attempts. If a system lock is activated, no users will be able to log in to Slingshot. A system lock does not remove active users who currently have active sessions with the server.

Lockout Rules Configuration

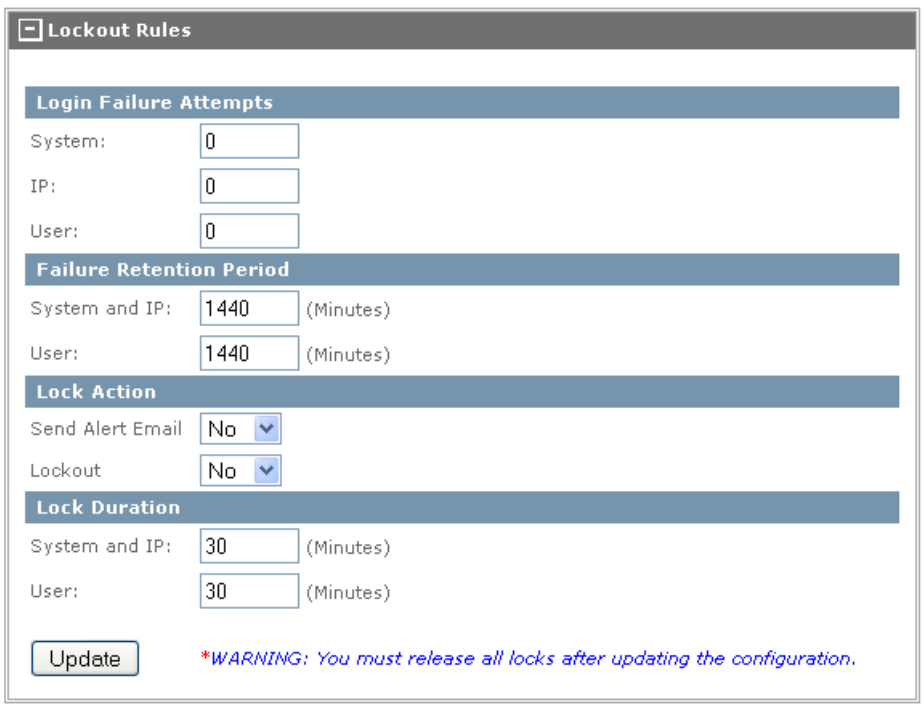


Figure 15

There are three types of lock out rules that can be configured:

1. Lock out users after a defined number of invalid login attempts

2. Lock out an IP Address after a defined number of invalid login attempts

3. Lock out of the entire System after a defined number of invalid login attempts

In addition, you can define how long invalid login attempts are retained in the system, and how long a user, system or IP will be locked out. The "Lock Action" parameters define whether the System, IP, or User will be locked out, and whether a notification email will be sent to an Admin. Note that the intent of the Lock Out parameters is twofold:

1. To lock out a user or IP Address and block additional login attempts when pre-defined thresholds are exceeded.

2. To notify an admin when predefined thresholds for invalid logins are exceeded.

Note: Users already logged in will not be affected.

The Lockout rules are broken up into four sections:

1. Login Failure Attempts
2. Failure Retention Period
3. Lock Action
4. Lock Duration

Super admins restricted to login from a designated IP will never be locked. It is recommended that customers either replace the default super admin account (UserID=admin) with an obscure user ID, or restrict super admin account to a particular IP addresses. This is to ensure the super admin's continued access to the system. If a super admin's attribute is changed or if additional super admins are added, the admin should release all locks for the change to take effect. Restarting the system automatically release all locks.

Each section will now be discussed in more detail.

Login Failure Attempts defines the maximum number of failed login attempts before any action will be taken. After this threshold is reached, login can be disabled for the number of minutes defined by the "Lock Duration". Note that these parameters and the "Failure Retention Period" parameters are closely related. These parameters should be set high enough so that this number is higher than the normal number of invalid login attempts for within the Retention Period defined.

System defines the maximum number of failed login attempts for the entire system. After this threshold is reached, login to the system can be disabled for the number of minutes defined by the "Lock Duration: System and IP". Allowed values are from 0 to 999999. A value of 0 means that there is no limit for the number of invalid login attempts for the System.

IP defines the maximum number of failed login attempts for an individual IP Address. After this threshold is reached, login to the system from the IP Address can be disabled for the number of minutes defined by the "Lock Duration: System and IP". Allowed values are from 0 to 999999. A value of 0 means that there is no limit for the number of invalid login attempts for an IP Address.

User defines the maximum number of failed login attempts for a user. After this threshold is reached, login to the system for that user can be disabled for the number of minutes defined by the "Lock Duration: User". Allowed values are from 0 to 999999. A value of 0 means that there is no limit for the number of invalid login attempts for a User.

Failure Retention Period defines how long invalid login attempts for the System, IP Address and a User are retained. Note that locks can be released by the Management ==> Lockout Management page or when the system is restarted.

System and IP defines how long invalid login attempts for the System and an IP Address are retained. The default value of 1 indicates that invalid login attempts are retained for 1 minute. Valid values are from 1 to 1440 minutes.

User defines how long invalid login attempts for the User are retained. The default value of 120 indicates that invalid login attempts are retained for 120 minutes. Valid values are from 1 to 1440 minutes.

Lock Action defines the actions that will be taken when the Login Failure Attempts thresholds are reached within the Failure Retention Period. Two options are Available:

Send Alert Email defines if an alert email will be sent to the email address defined by the "Send Alert Email To" parameter defined on the "Slingshot Configuration" page. If a valid email address is not configured on that page, no email will be sent.

Lockout defines that the User, IP Address or System will be locked out. The amount of time that a user, IP Address or System will be locked out depends on the "Lock Duration" settings.

Lock Duration defines the number of Minutes that the System, IP Address or User will be locked out. Note that locks can be released by the Management ==> Lockout Management page or when the system is restarted.

System and IP defines the number of Minutes that the System or an IP Address will be locked out. The default value of 5 indicates that the System or IP Address will be locked out for 5 minutes. Valid values are 0 through 1440. The value 0 means that the System or IP Address will not be unlocked automatically; the admin must manually unlock the System or IP.

Users defines the number of Minutes that the User will be locked out. The default value of 30 indicates that the User will be locked out for 30 minutes. Valid values are 0 through 1440. The value 0 means that the User will not be unlocked automatically; the admin must manually unlock the user.

Note that when the Lockout Rules parameters are changed, you must release all locks or restart the system.

Administrator Lockout

To ensure that the administrator user can not be locked out, follow the steps below:

1. From the Administrator page, navigate to ‘Users > Manage Users’. Find the administrator account and click on the UserId to edit that account.

2. Expand the ‘Optional User Properties’ dropdown menu.

3. Under the section ‘Restrict User Login by IP Address or IP Name’, enter your IP address into the ‘IP Address or IP Name’ field.
4. Check the box that says ‘Restrict User’.

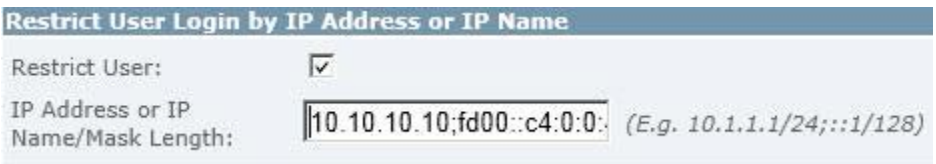


Figure 16

5. Your administrator user is now restricted by IP address. The admin will only be able to log in from the IP address that has been associated with the user. Login attempts from any other IP address using the administrator user will be blocked.

Note: If the administrator does become locked out, restarting the web server will release all locks.

Setting up an Alert Email

If the option 'Send Alert Email' is set to yes, the administrator will receive an email notification whenever a lockout occurs. This email address is entered in the Slingshot configuration page found at Management > Slingshot > Configuration.
Use the field "Send Alert Email To:" to configure the email address that will receive lockout alert notifications.

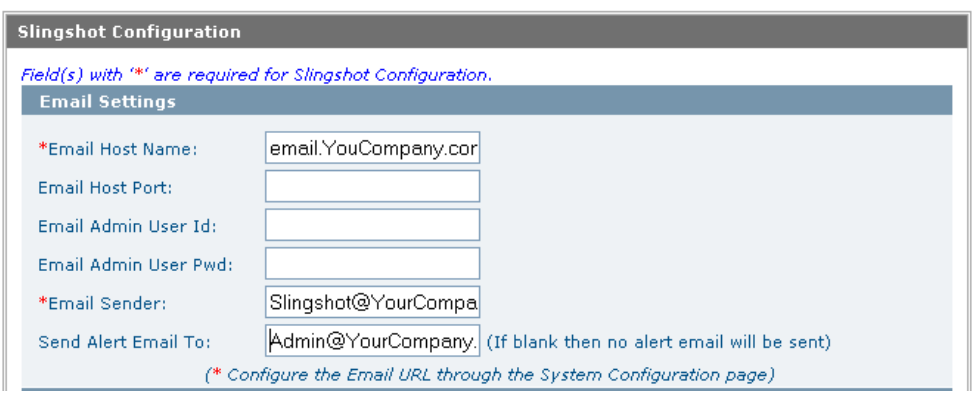


Figure 17

PGP Settings

This box defines the Global PGP settings that will be used by the Slingshot Server.

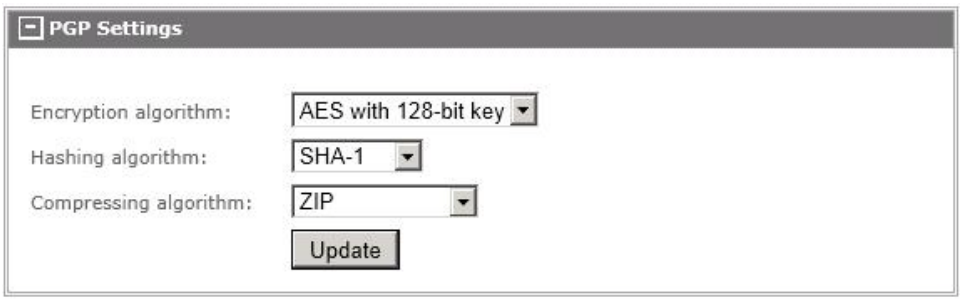


Figure 18

In the table below we will discuss each parameter that can be set for this Slingshot servers **PGP Settings** window:

Parameter	Description
Encryption Algorithm	The Encryption Algorithm that will be used for PGP Encryption for this Slingshot server.
Hashing Algorithm	The Hashing Algorithm that will be used for PGP Encryption for this Slingshot server. Note: Bouncy Castle only supports signatures using a DSA signing key with hashing algorithm SHA. If are using an RSA signing key any of the hashing algorithms can be used.
Compression Algorithm	The Compression Algorithm that will be used for PGP Encryption for this Slingshot server.

Slingshot Configuration

Navigation: Management > Slingshot > Configuration

Below we discuss the Slingshot configurations by their 5 associated sections.

Email Settings

In the *Email Settings* section, any field name that is marked with a red asterisk (*) is required for the configuration to be completed. These fields are all you need to configure for Slingshot to run successfully:

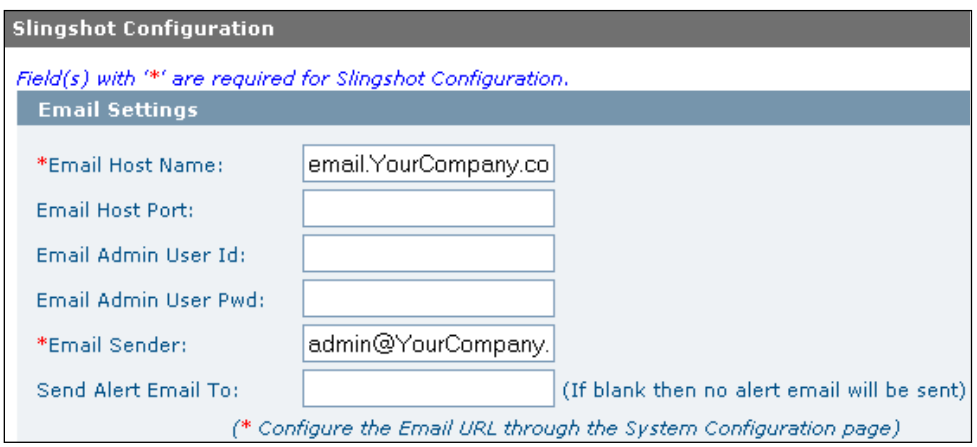


Figure 19

Parameter	Description
Email Host Name	Your email server's IP or host name
Email Host Port	The port your email server is listening on. Defaults to port 25 if left blank.
Email Admin User Id	This field is used when your Email Server requires a User Id and Password for authentication.
Email Admin User Pwd	This field is used to hold the password for the Email Server User Id for authentication.
Email Sender	The senders email address that will be used and displayed to new users added to the Slingshot system via email, when a Password Reset is requested, or Self Registration is enabled.

Parameter	Description
	Note: Users should not be able to respond to this email address.
Send Alert Email To	Defines the admin email address where Slingshot will send Alert Emails. Alert Emails are sent when invalid login thresholds are exceeded for Users, IP Addresses and the System.

Repository Settings

The *Repository Settings* section holds the server name and the directory on that server that will be used to house the files being sent and received by Slingshot users. By default this is the Local web server, however if you have a MFT Platform Server installed on a Windows or UNIX system you can have the files moved to one of these systems instead. (See Add Server for more information.)

Figure 20

Warning: If you are using a MFT Platform Server for your repository and/or Vault server it is not recommended changing the Server definition. For example setting PGP keys for the MFT Platform Server where they were not used in the past.

Settings for Users Created by Senders

This section controls how new user accounts will be created when they are added to Slingshot via an email sent via the Slingshot Browser Interface. Only Full and Power users can create new user accounts (See User Type in the Add User section for more information).

Figure 21

Parameter	Definition
User Visibility	When a new user is added to the system will there visibility be public or private. For more information on visibility see the Add User section.
Internal E-mail Domains	Internal domains located within your production environment. Allowed Values: ALL, NONE, or 1 or more internal domains. i.e. yourcompany.com
Create Users in External E-mail Domains	Determines whether or not a new user in an external domain can be created via email. For example: user@yahoo.com
Initial User Status	Will the new user's account be enabled or disabled when it is added?
Guest User Expiration	The amount of days a Guest user account will be active.
Guest User Reactivate	When enabled a Guest user account can be reactivated when a new Slingshot email is sent to them.

Settings for Slingshot Outlook Plug-in

You can configure the Slingshot Outlook Plug-in to follow a set of rules when users send file attachments via Outlook. The table below describes the rules displayed in Figure 19:

Figure 22

Parameter	Definition
Rules	Do you want the Transfer Size Rules and the Attachment Type Rules to be enforced or suggested when a user clicks the Outlook Send button. Enforced Rules – This will cause the user to have to send out the email attachments via Slingshot. Suggest Rules – Prompts users with a choice of sending the file attachment with Slingshot or Outlook.
Transfer Size Rule	An email with file attachment(s) being sent via Outlook cannot 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 Type 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).
Single Sign-On	This option defines whether the Outlook Plug-in will use SSO (Single Sign-On). Users will sign-on once with their existing Slingshot password which will then be encrypted and saved as a token in the database. From that point on the user will not be prompted again for a new password. This includes LDAP user as well as the Slingshot database users. Note: If the Single Sign-on option is Disabled at a later date only new users will be affected by this change. Existing users will continue to be logged in as Single Sign-on unless the token saved in the database has been removed.

Slingshot Settings

This section is used to configure the default values for email file attachments being sent via Slingshot Web Browser Interface or the Outlook Plug-in.

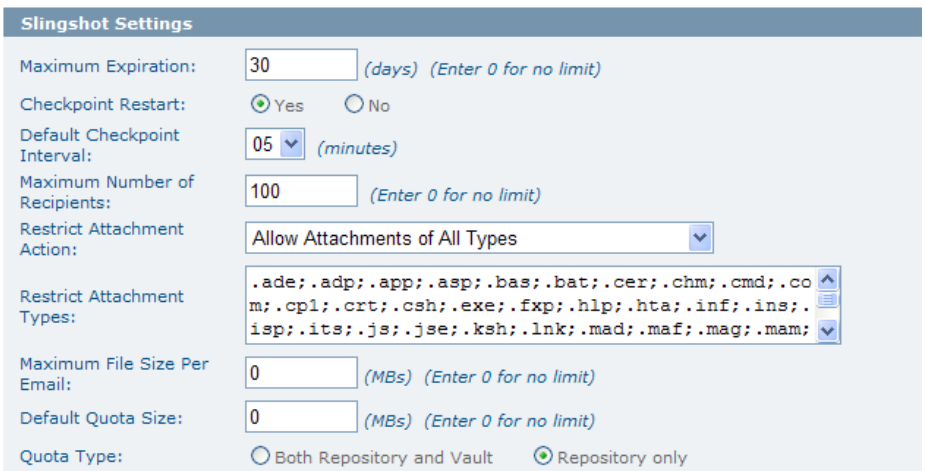


Figure 23

Parameter	Definition
Checkpoint Restart	Enabled a checkpoint to be taken at the checkpoint Interval during an email file attachment send or receive with the Slingshot Outlook Plug-in and on an email receive only with the Slingshot Browser Interface 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 from being sent. You can choose to follow Outlook's rules, follow our defined list in the Restrict Attachment

Parameter	Definition
	Types field or use a combination of both.
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 SV.
Default Quota Size	Global setting that controls the amount of disk storage available to all Slingshot users. If this value is set to 100, every Slingshot user will have 100MB of their own disk storage space available for sending attachments. The default is 0 for no limit.
Quota Type	Both Repository and Vault: Both active and archived attachments will be counted against a user's disk quota. Repository Only: Only active attachments that have not expired will be counted against a user's disk quota.

Archive Server Integration

This box defines settings used by the Slingshot Archive Server interface. Slingshot has the capability of forwarding all requests to an Email Archive Server. This box defines the settings for enabling and configuring this capability.

Email Archive Status: defines whether the Archive Server is enabled. There *are three possible settings:*

Enabled Real Time: tells Slingshot to forward requests to the Email Archive Server in real time. If a request fails, it will be retried in batch mode. *This is the suggested setting.*

Enabled in Batch: tells Slingshot to forward requests to the Email Archive Server in batch mode. Since Batch Mode runs in the Slingshot Vault Server thread, Batch Mode requires that the Slingshot Vault Server be enabled. Note that it is less efficient than "Enabled in Real Time". *Real*

Time and should be used when you want the requests archived during off-peak hours.

Disabled: tells Slingshot that requests should not be forwarded to an Email Archive Server. *This is the default setting.*

Email Archive Host Name defines the host name or IP Address of the Email Archive Server. There is no default for this parameter. If the Email Archive Status is set to Enabled Real Time or Enabled in Batch, this parameter is required.

Email Archive Host Port defines the IP Port of the Email Archive Server. If not entered, this parameter will default to port 25.

Email Archive Admin User Id defines the User ID that will be sent to the Email Archive Server. Note that this parameter is optional and is only required when the Archive Server requires User Id and Password authentication.

Email Archive Admin Password defines the Password that will be sent to the Email Archive Server. Note that this parameter is optional and is only required when the Archive Server requires User Id and Password authentication.

Max Retry Days defines the how long a failed Archive Server request will be retried. When first enabled, this parameter also defines the age of requests that Slingshot will archive. The default value is 30. This means that Slingshot will retry requests for up to 30 days. It also means that when first enabled, Slingshot will archive requests up to 30 days old.

Third Party Archive

When using a third party archive system with Slingshot, there will be two records stored in the archive repository every time a Slingshot message is sent. See example below:

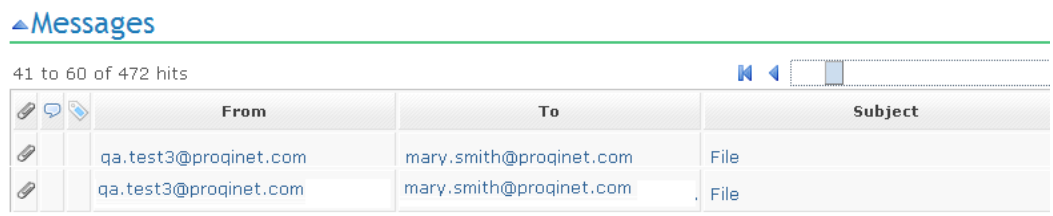


Figure 24

One record will contain the message text that passed through the email server with the original email message replaced with the Slingshot.txt file.

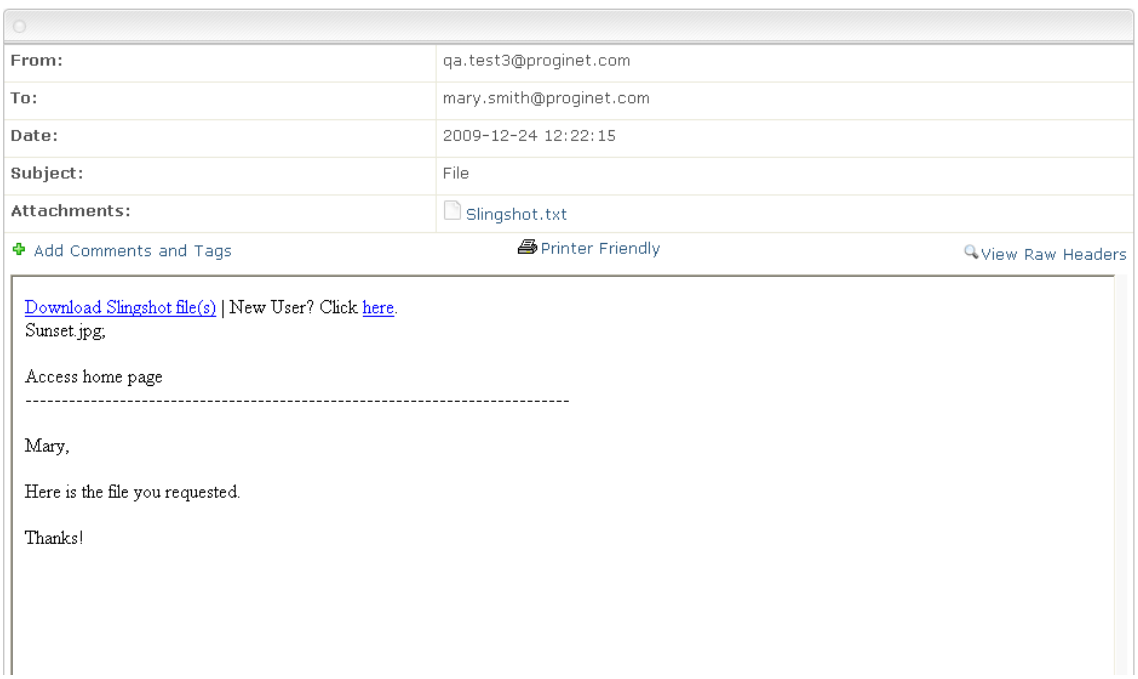


Figure 25

The second record will contain the original message text and original attachment sent from Slingshot.

Vault Server Settings

The Vault Server is responsible for moving files from the repository to an archive location located either in a directory on the local web server or on a MFT Platform Server installed on either a Windows or UNIX system. The Vault server will scan for file attachments that have expired and

move them from the repository to this location for storage. Only the sender can access these files.
Warning: If you are using a MFT Platform Server for your repository and/or vault server it is not recommended changing the Server definition. For example setting PGP keys for the MFT Platform Server where they were not used in the past.

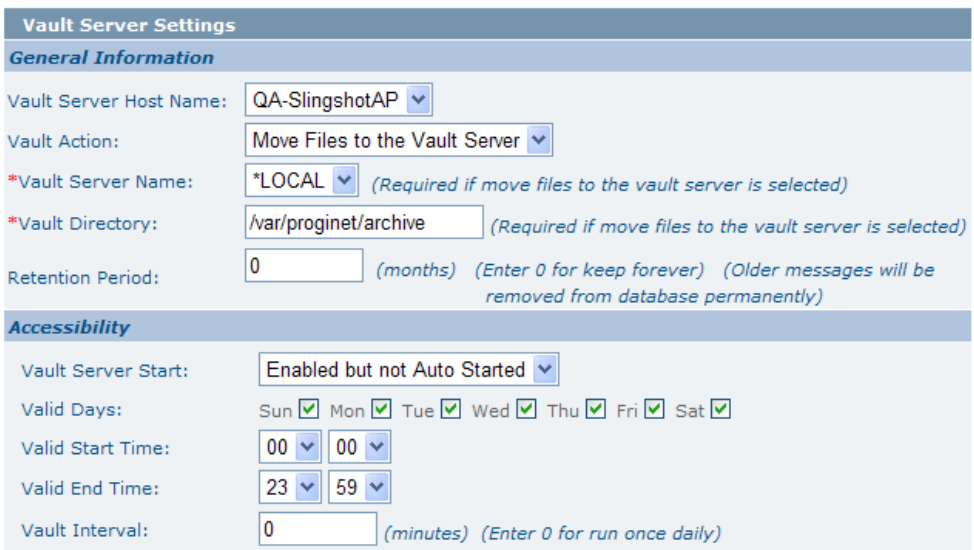


Figure 26

In the tables below we will discuss the Vault Server Settings broken out in the two sections, *General Information* and *Accessibility*:

General Information

Parameter	Definition
Vault Server Host Name	The Slingshot host server name (not configurable)
Vault Action	When Slingshot scans for files that have expired do you want to Move them to an Vault Server location or delete them?
Vault Server Name	The name of the server where the files will be archived too. By default it is the local web server. You can configure a MFT Platform Server to be used

Parameter	Definition
	in the Add Server web pages.
Vault Directory	The directory where files will be placed. i.e. c:\ArchivedFiles
Retention Period	How long do you want to retain the file attachment audit information in the database?

Accessibility

Parameter	Definition
Vault Server Start	By default the Vault server is set to Enabled but Not Auto Started. This means that the Vault server must be started manually by navigating to Management>Slingshot>Vault Server Status web page and clicking on the Start Server 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.
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 between the Valid Start Time and Valid End Time.

Vault Server Status

Navigation: Management > Slingshot > Vault Server Status

Figure 27

The Slingshot Vault Server Status allows you to see the current status of the Slingshot Vault Server. As you can see in Figure 22 you can see our server status reporting it is in sleep mode. You can also stop and start the Vault server from this web page as well.

Alerts

Alerts allow you to perform an action based on the completion of a Slingshot email. Alerts can be triggered by setting the **Alert Trigger Criteria**. Up to four different alert actions can be triggered based on the Alert Trigger Criteria. More than one alert can be triggered for the same Slingshot email.

Add Alert

Navigation: Management > Alerts > Add Alerts

Figure 28

First you want to give your Alert a unique name and set the severity of the alert (this is for informational purposes only).

Then you would setup what function will take place for this alert to be triggered by filling in Alert Trigger Criteria as seen in our example in Figure 24 below:

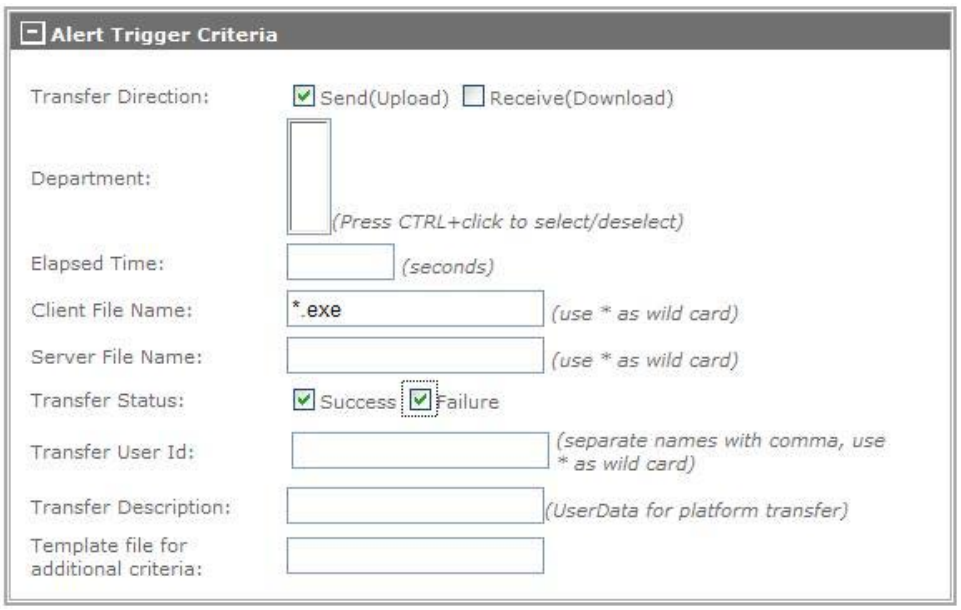


Figure 29

Last you would choose what action will take place upon the alert being triggered. You can choose to have an email sent to someone (Figure 25), a SNMP Trap to be sent (Figure 26), have a command executed (Figure 27), and/or execute a JAVA Class you have (Figure 28).

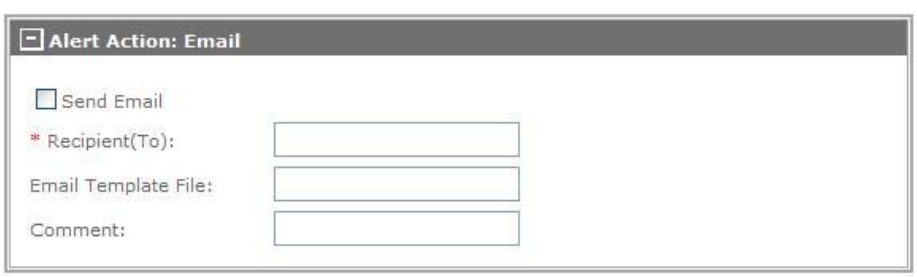


Figure 30

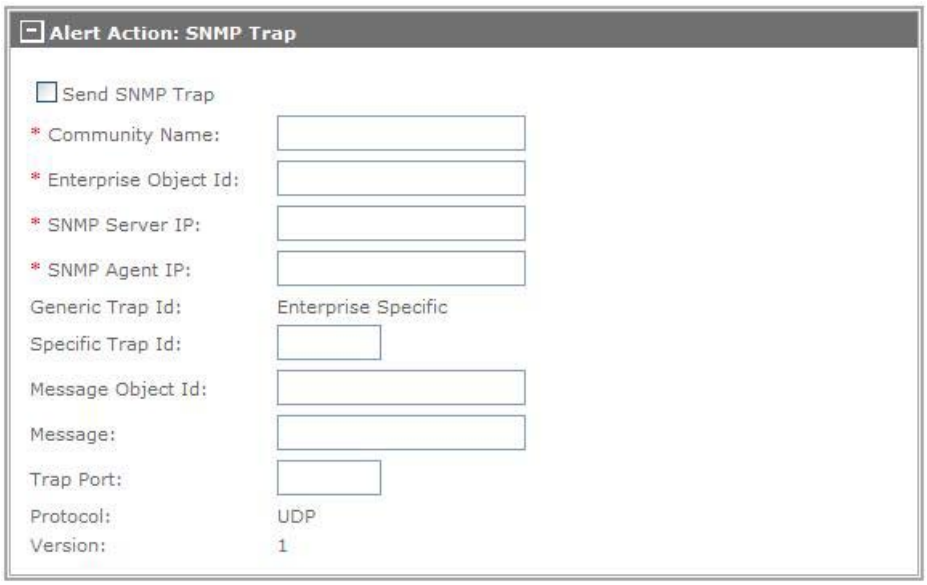


Figure 31

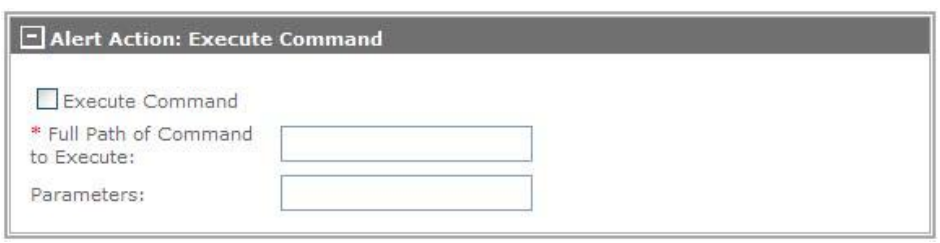


Figure 32

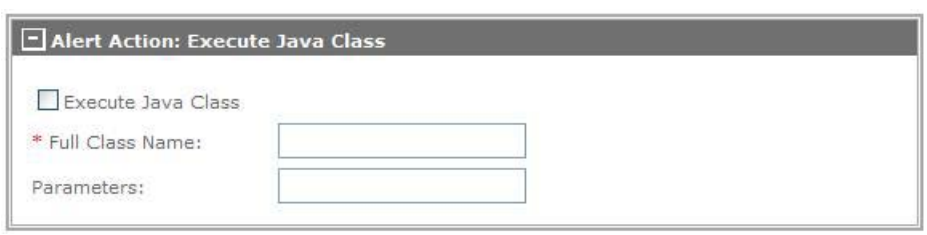


Figure 33

The table below describes each Alert Action parameter from Figures 25 – 28:

Parameter	Definition
Send Email	Enable this box to activate the Email action
Recipient To	The email address(s) an email will be sent to when this alert is triggered. You can define multiple email addresses by separating them with a comma.
Email Template File	When an email is sent Slingshot uses an email template to format the email being sent out. By default Slingshot will use the email template file “email-alert-notification-template.xml” contained in the (WEB_HOME)\ webapps\cfcc\email-template directory. So this field can be left blank. If you want to define a different xml file you can write the xml file name here however you must place your xml file in the email templates default directory.
Comment	This will place a comment in the email that would be sent out.
Send SNMP Trap	Enable this box to activate an SNMP trap to be sent out as the alert action.
Community Name	This is a required field, although most customers specify the Community Name as "public"
Enterprise Object Id	You can put any valid Object Id into this field; however, the Enterprise ID for TIBCO is 1.3.6.1.4.1.2938.2.1.1 and should be used if you do not have a specific Enterprise Object ID.
SNMP Server IP	The SNMP Server (Manager) IP Name or IP Address of the SNMP Trap Server where the traps will be sent.
SNMP Agent IP	The Source Address for the SNMP Trap. You should define the Slingshot Server IP address if no other enterprise SNMP software is in use.
Generic Trap Id	Not configurable.
Specific Trap Id	The trap id should be defined as an integer and is

Parameter	Definition
	used to uniquely define the SNMP Trap.
Message Object Id	Typically this parameter uses the Enterprise Object Id as a prefix and adds a suffix to define the Message that is to be displayed in the Trap. Given the TIBCO Enterprise Id, a suggested value for this parameter is 1.3.6.1.4.1.2938.2.1.1.11.
Message	Contains the message that is sent to the SNMP Server (manager) within the SNMP Trap. You should define any text information that describes the problem here.
Trap Port	The IP Port used for Trap requests. Port defaults to 162.
Protocol	Not configurable.
Version	Not configurable.
Execute Command	Enable this box to activate the execution of a command to be run as an alert action.
Full Path of Command to Execute	The exact path, including directory and file name, of the command that you want to execute.
Parameters	Defines the command line parameter(s) if needed for the executing command. This parameter accepts the same tokens as the email template.
Execute Java Class	Enable this box to activate the execution of a Java Class to be run as an alert action on the Slingshot J2EE server. Note: that when the Java Class executes, it is executed under the UserID associated with the J2EE server. For this reason, this action is not available to Department Administrators. A sample Java Class is distributed with the Command Center with the following name: ....\example\UserJavaclassExample.java
Full Class Name	This parameter value holds full class name with package name, for example, com.abc.Test. After the Slingshot Server installation on web server

Parameter	Definition
	complete, there will be a sample Java source file UserJavaclassExample.java under the “example” directory. Follow Java's requirement to compile the class file. The interface com.proginet.cfcc.auditManager.alerts.AlertActionIF is located at ...WEB-INF\classes\com\proginet\cfcc\auditManager\alerts; under the application context of the web server.
Parameters	Defines a string passed into the doAction method for Execute Java Class action. This parameter accepts the same tokens as the email template.

Manage Alerts

Navigation: Management > Alerts > Manage Alerts

The Manage Alerts page allows you to list and update Slingshot Alerts. The Manage Alerts page displays the first 100 Alerts defined. If you click on the Alert Id of an entry in this table, a detail page will be displayed that allows you to update the entry if you are authorized. If more than 100 entries are returned you can view the next 100 entries by clicking on List Next 100>. To delete Alerts, click on the check box to the left of the Alert Id and click on the Delete button.

Keys

PGP Public Keys

Public PGP keys can be used to encrypt files being emailed by a particular user or for a MFT Platform Server being used to house the repository or archive files. You can add and manage the public PGP keys from this location.

Add PGP Key

Navigation: Management > Keys > PGP Public Keys > Add PGP Key

Figure 34

From the Add PGP Keys page the administrator would associate a PGP public key with a particular Slingshot user or a MFT Platform Server that was defined. Once you have pasted the PGP public key in its base64 format (seen below in our Example PGP base64 format) into the box provided and selected either the user or server you want to use then click on the **Continue** button to add the public key to the Slingshot database. You will be prompted to confirm you want to add this PGP key to the database. Only one key can be associated with a user or server at a time. By default the status of the key is set to Disabled unless changed.
Example PGP base64 format:

-----BEGIN PGP PUBLIC KEY BLOCK-----
.....pgp key information.....
.....pgp key information.....
-----END PGP PUBLIC KEY BLOCK-----

Mange PGP Keys

Navigation: Management > Keys > PGP Public Keys > Manage PGP Keys

The Manage PGP Keys page allows you to list and update, the PGP public key definitions. The Manage PGP Keys page displays the first 100 PGP keys records defined. It also gives you the capability to search the database to limit the number of PGP keys definitions displayed.

Selection Criteria

This box allows you to selectively search the PGP key database to limit the number of records that are displayed. The % character is used as a wildcard character to simplify the search. If a field has no search criteria entered, then no filtering will be done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a record will be returned. When you have completed the Search Criteria, click on the Search button. The output will be placed in the Results table. Up to 100 PGP keys will be displayed at a time within the Results table. If more than 100 entries are returned for a search, you can view the next 100 entries by clicking on List Next 100>. If you click on the Key Type of an entry in this table, a detail page will be displayed that allows you to update the PGP public key configured if you are authorized.

PGP System Keys

If you want to add another layer of security to your Slingshot environment you can create PGP System Keys (aka Private key) to be used to decrypt PGP encrypted files emailed via Slingshot. If you have a PGP private and public key already you can import them to be used for this purpose as well. If for any reason you need to make a change to these keys you can manage them from this location as well.

Create PGP Key

Navigation: Management > Keys > PGP System Keys > Create PGP Key

From the Create PGP System Key page the administrator would fill in the desired criteria he/she would like the key created with and then click on the **Create Key** button to add the System key to the Slingshot database. By default the first key ever to be created or imported into the database will be set as the Default Key. There after you must enable the Set as Default Key box for any new key you create if you want it to be the default key used.

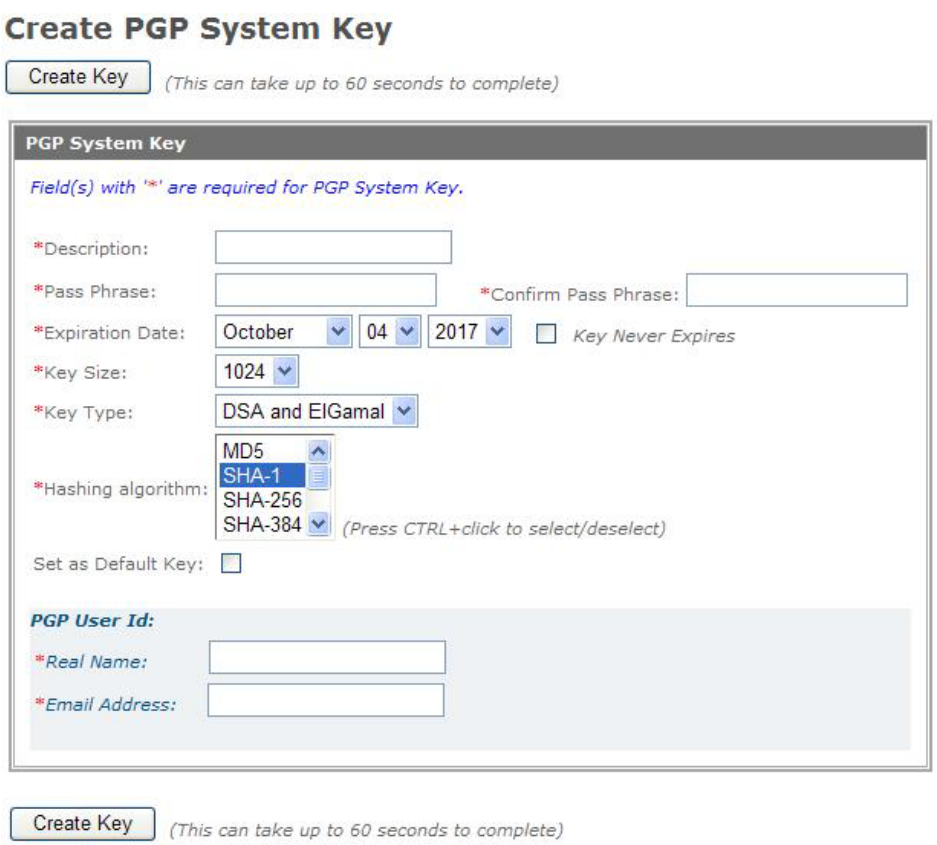


Figure 35

Below is a description for all the parameters available to be set as seen in Figure 30 for the Create PGP System Key page:

Parameter	Definition
Description	A unique description given to a PGP System key to distinguish it from others.
Pass Phrase	A word or phrase to be used to decrypt PGP files with.
Confirm Pass Phrase	Confirm the pass phrase you used in the “Pass Phrase” field
Expiration Date	The date you want the PGP System Key to expire. Default is 5 years.
Key Never Expires	Enable this checkbox if you want your PGP key to never expire.
Key Size	Set your key to be either a 1024 bit key or 2048 bit key.
Key Type	Set the digital signature and key encryption algorithms.
Hashing algorithm	Set the preferred hashing algorithm. One or more hashing algorithms can be selected.
Set as Default Key	Set this PGP system key to be the default used by the system unless told to use another.
Real Name	Define a name that will be set for this PGP key. This can be a person’s name or a unique descriptive name for users to see.
Email Address	An email address that will be associated with this PGP system key.

Import PGP Key

Navigation: Management > Keys > PGP System Keys > Import PGP Key

If you have a PGP key pair already and would like to use it for as the PGP System Key you would import the key to the Slingshot database. In order to have a working imported key it must be generated by a PGP or gpg utility. If you want to create a key using a gpg utility you would execute the following command:

gpg --gen-key

After answering some configuration questions, this utility will create a secret key (secring.gpg) and a public key (pubring.gpg). To get the secret key and public key information separated so they can be copied into the Import PGP key web page, issue the following commands:

gpg --export -a >publickey.cfi 6

gpg --export-secret-key -a >secretkey.cfi

Now, edit the files and copy/paste the data into the fields marked PGP Secret Key and PGP Public Key. When the necessary parameters are defined, the user should click on the **Continue** button to import the PGP System Key to the Slingshot database. Note that before the Private Key is actually added to the Slingshot database a confirmation page will be displayed to verify that the information entered is correct.

Parameter	Definition
Private Key Pass Phrase	The imported key password (or pass phrase).
Confirm Pass Phrase	Confirm the imported keys password (aka pass phrase) you used in the Private Key Pass Phrase.
Set as Default Private Key	Set this PGP system key to be the default used by the system unless told to use another.
Description	A unique description given to this PGP key to distinguish it from others.
Enter the PGP Secret Key in the box below	Paste the secret key (aka private key) in base64 format into this box.
Enter the PGP Public Key in the box below	Paste the public key in base64 format into this box.

Manage PGP Key

Navigation: Management > Keys > PGP System Keys > Manage PGP Keys

The Manage PGP Keys page allows you to list and update, the PGP system key definitions. The Manage PGP Keys page displays the first 100 PGP keys records defined. It also gives you the capability to search the database to limit the number of PGP keys definitions displayed.

Selection Criteria

This box allows you to selectively search the PGP system key database to limit the number of records that are displayed. The % character is used as a wildcard character to simplify the search. If a field has no search criteria entered, then no filtering will be done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a record will be returned. When you have completed the Search Criteria, click on the 

button. The output will be placed in the Results table. Up to 100 PGP keys will be displayed at a time within the Results table. If more than 100 entries are returned for a search, you can view the next 100 entries by clicking on List Next 100>. If you click on the Description of an entry in this table, a detail page will be displayed that allows you to update the PGP system key configured if you are authorized.

Activity

Active Users

Navigation: Management > Activity > Active Users

Figure 36

This page displays all the active sessions in the system. In our example above you can see the admin's session currently running. By default Slingshot will hold a user's session for 8 hours before it will timeout. Your web server's default timeout maybe different. Depending on which one comes first the user's session will expire, however their session id will remain active for the 8 hours unless the Slingshot timeout is changed in the web.xml to match that of your web servers.

To delete a user's session, select the check box next to the session that you wish to delete and click on the Delete button at the bottom of the panel. Multiple sessions may be deleted at one time.

Internet Checkpoints

Navigation: Management > Activity > Internet Checkpoints

The Internet Checkpoints section contains all the checkpoints for all the emails done through the Slingshot Outlook Plug-in and for email file attachments downloaded through the Slingshot Browser Interface set in Java mode. Only when running a Browser Interface download set to Java mode is Checkpoint Restart used. The user must have **AdministratorRight** in order to manage checkpoints.

A listing of particular Checkpoints can be obtained by entering the search criteria for any combination of the following: Transfer Id, User Id, Client File Name, Node Name, Server File Name, Transaction Id and Proxy Transaction Id. A percent sign (%) may be used a wildcard character.
To delete a Checkpoint, select the check box next to the Checkpoint that you wish to delete and click on the Delete button at the bottom of the panel. Multiple checkpoints may be deleted at one time.

Authenticators

Add Authenticator

Navigation: Management > Authenticators > Add Authenticator

In order to pull in users from an LDAP Server to Sync with the Slingshot database you need to configure what we call an Authenticator for communication to take place between Active Directory and the Slingshot Server. The authenticator configuration is broken up in four sections. We will discuss each section as they are seen on the web page. First set the Authenticator Name that will be used. Note: This is the qualifier name and will be included as a prefix before each LDAP user id that is pulled into the system. However, the end user will NOT need to include the qualifier name with their user id when they are logging in to the system.)

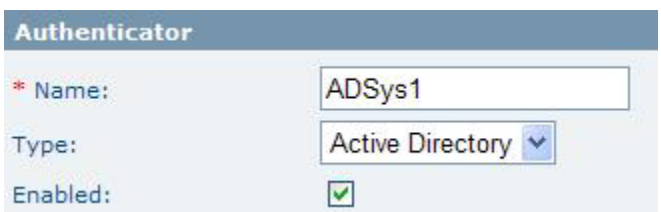


Figure 37

Parameter	Definition
Authenticator Name	The authenticator name does two things. Gives this LDAP a unique name from any others that may be used and is prefixed to the user's id with a dash when it is pulled in from the LDAP server. Ex. serverA-john.doe Note: A dash "-" or embedded spaces should not be used in the name. Warning: This field cannot be modified later.
Directory Type	Active Directory or Database can be set. For more information regarding use of a database please refer to section Database Authenticator Configuration.

Enabled	Enables or Disables this LDAP Authenticator. If this box is disabled all users connected to this LDAP server will no longer be able to connect to Slingshot.

Below we will discuss the LDAP Server Connectivity section which defines the parameters necessary to connect to the LDAP Server.

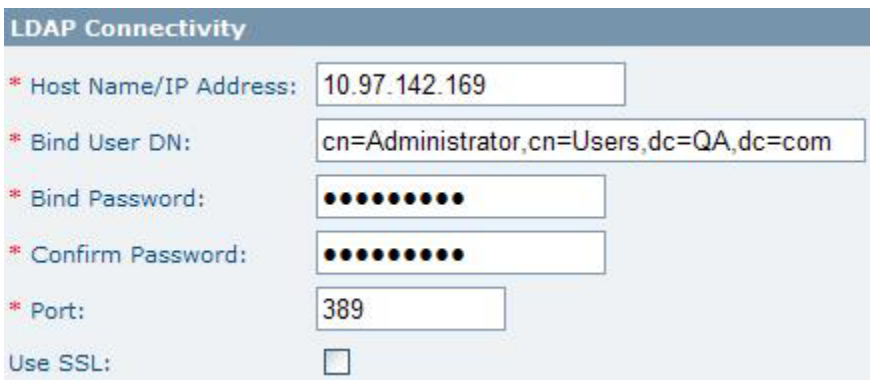


Figure 38

Parameter	Definition
Host Name/IP Address	IP Name or IP Address of your LDAP server.
Bind User DN	The distinguished name (DN) required for authenticating to the LDAP Server.
Bind Password	The password associated with the Bind User DN.
Confirm Password	Confirming the password associated with the Bind User DN.
Port	The default LDAP port used by your LDAP server. Non-SSL requests are generally 389, and port 636 is used for LDAP SSL.
Use SSL	If your LDAP server is using SSL you must enable this box.

The LDAP Search section is where you define the LDAP properties in order to find your user accounts to sync with the Slingshot database.

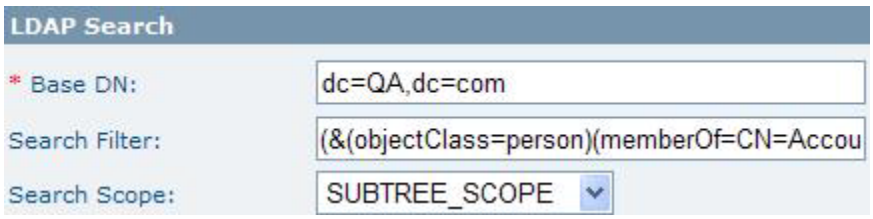


Figure 39

Parameter	Definition
Base DN	The base in the LDAP tree where all Slingshot users are defined. The levels searched below this base depend on the Search Scope parameter.
Search Filter	The LDAP Search Filter that is used for LDAP User searches. The default value should be used unless otherwise instructed by Technical Support
Search Scope	The LDAP levels below the Base DN that will be searched. There are three possible values: SUBTREE_SCOPE - defines that all levels below the Base DN will be searched. This is the default value and should be used by most users. ONELEVEL_SCOPE - defines that only the level defined by the Base DN will be searched. OBJECT_SCOPE - defines that only the object defined by the Base DN and the Search Filter will be searched. This should only be used when instructed by Technical Support.

The LDAP Attributes section contains the attribute values that have been predefined for you. The default attributes are those used by Microsoft Active Directory LDAP server unless they have been changed. If an attribute is different than change the value.

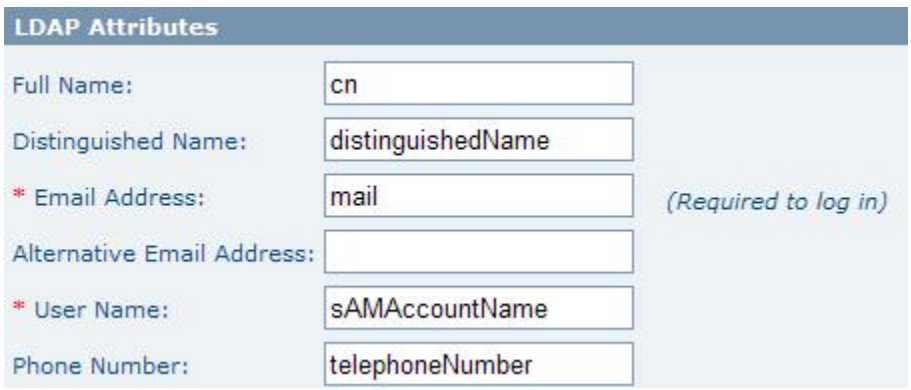


Figure 40

Once you have completed configuring your authenticator simply click the Add button to have it added to the system. This will allow you to run an LDAP Sync to pull in your AD users. However, we recommend testing your configurations before running the LDAP Sync. Please refer to the Manage Authenticators section for more information regarding testing y our authenticator settings.

Note: In a multi-server environment, Slingshot LDAP Authenticator names should be identical on each server.

Manage Authenticators

Navigation: Management > Authenticators > Manage Authenticators

The Manage Authenticators page lists the Slingshot LDAP Authenticators defined to the system. From here you can delete, test or edit your LDAP authenticator(s).

To delete an authenticator simply click on the box in the Delete column of the one you no longer need to select it and then click the Delete button.

If you need to test an authenticator's connection you would click on the Test link.

To edit an authenticator's configurations you would click on the **Authenticator Name** for the one you want to change and a details page will open for you to make your configuration changes.

Database Authenticators

Database Authentication should only be used in a multi server, multi database Slingshot environment. Database authenticators can be used in conjunction with LDAP authenticators to ensure that user records remain identical across all servers and databases.

Once a database authenticator has been set up for each of your Slingshot servers, users who are not LDAP synced will be able to access every server in your environment, regardless of which server and database that the user was originally created on.

Configuration:

The administrator must choose one Slingshot server that will act as the authentication database for all other servers. This server's database will serve as the primary database in your environment. It will provide authentication for any server that has a database authenticator connected to the primary database.

Only one database authenticator can be configured for each individual server in your environment. The server where your primary database is located should not have a database authenticator configured. On all secondary servers, the database authenticator connection properties should be identical. For example, in a three server environment:

#	Server Name	Database	Database Authenticator Configuration
1	Server A	Primary	None
2	Server B	Secondary	Connect to Server A's Primary database
3	Server C	Secondary	Connect to Server A's Primary database

Configuring a database authenticator on secondary servers:

Figure 41

Database Connectivity:

This section is used to define the connectivity information required to make a JDBC connection to the Authentication Database. The only purpose of the authentication database is to serve as a central storage for user IDs and passwords. It will not be used for other purposes unrelated to matching ID and password. For example, features like disable and delete users will continue to be managed and only within the application's primary database. In addition, password rules should be the same on all databases. The user ID and password synchronization only takes place between the centralized database and the application's primary database. There is no automatic synchronization among all databases. Only user ID and password will be synchronized. It is possible that an old user's password exists in a Slingshot database. To prevent user from logging in using an old password in a local database, configure Slingshot to check the centralized database first and only.

Parameter	Definition
DBConn	Defines the connectivity information necessary to connect to the Authentication database. To get this information, open a Slingshot Admin browser window to the Slingshot Server that uses the Authentication Database. Go to the Reports -> Diagnostics page and search for the parameter "DBConn" in the "web.xml Context Parameters" section. Copy the data starting with "jdbc..." and enter this information in this field. Note that if DBCONN defines a Host name of localhost or 127.0.0.1, the actual IP Address or IP Name should be

Parameter	Definition
	substituted.
JDBC Driver	Defines the JDBC Driver information necessary to connect to the Authentication database. To get this information, open a Slingshot Admin browser window to the Slingshot Server associated with the Authentication Database. Go to the Reports -> Diagnostics page and search for the parameter "DBDriver" in the "web.xml Context Parameters" section. Copy the data starting with "com... or net..." and enter this information in this field.
UserID	Defines the User Id required to authenticate to the Authentication Database.
Password	Defines the password associated with the User ID.
Confirm Password	Confirms that the password entered is correct. This field must exactly match the Password entered.
Check This Database	Defines the order that this database will be checked for authentication requests. The following options are allowed: : **First** defines that the Authentication Database is checked before the Slingshot Server database : **Last** defines that the Authentication Database is checked after the Slingshot Server database : **Only** defines that the Authentication Database is checked and that the Slingshot Server database is not checked

LDAP

LDAP Sync

Navigation: Management > LDAP > LDAP Sync

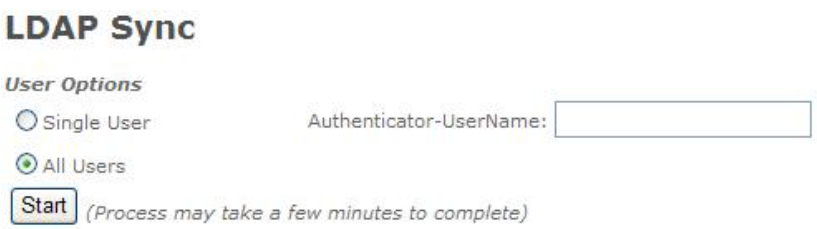


Figure 42

The LDAP Sync utility pulls LDAP user information defined to an LDAP server with corresponding users in the Slingshot database. To perform an LDAP Sync, the Slingshot Administrator must define an Authenticator per LDAP Server being used. See the Add Authenticator section for more information on adding an Authenticator to the Slingshot system.

During an LDAP Sync, the following parameters will be set for the user in the Slingshot database:

1) UserID
2) Full Name
3) Primary Email Address
4) Telephone Number

Warning: All LDAP users being synced to the Slingshot database must have an email address defined for them or they will not be entered into the database.

Most changes to a user's account will be done through the Manage Users web page. However if the user's account is managed by LDAP you will not be able to edit any of the LDAP Sync fields listed above. Any other field can be changed and when you perform the next LDAP Sync no changes will occur to the fields you changed.

Warning: In a multi-server environment any changes to an LDAP user's account via the LDAP server would require you to run the LDAP Sync for all your LDAP Authenticators defined.

You can sync a single user's account by selecting Single User and typing in the user's Slingshot user name and clicking on the Start button. Otherwise you can leave All Users selected and click the Start button. It will only sync new users or any user's account that has been updated. If for any reason an LDAP user should fail to sync with Slingshot you will be notified at the end of the sync process on the web page. You can read more about the reason why a user's account failed to sync by reading your **ldap_api_messages-mft-xxxxx.txt** file located in your Slingshot installation directory in the messages folder.

Lockout

Lockout Management

Navigation: Management > Lockout > Lockout Management

Figure 43

When a user, IP or system lock occurs, the lock will remain until the duration set on the 'Lockout Rules' page has been reached. An administrator can choose to bypass the configured lock duration period and manually release any lock. The Lockout Management page serves as a centralized location to release user, IP and system locks.

There are three types of locks that can be released, each of which has two options. Note that you can only select one of the six radio buttons at a time.

Lockout	Description
User	Allows you to release a lock for one or more users. The User Id(s) whose locks will be released must be entered in the box to the right. To release locks for more than one User Id, delimit the User Id(s) with a semi colon. All User IDs allows you to release all user locks

IP Address	Allows you to release a lock for one or more IP Addresses. The IP Address(es) whose locks will be released must be entered in the box to the right. To release locks for more than one IP Address, delimit the IP Address(es) with a semi colon. Note that IP Addresses must be entered in dotted decimal format and that IP Names are not allowed. All IP Address allows you to release all IP Address locks.
System	Allows you to release all System locks. All Locks allows you to release all User, IP Address and System locks. Note: Restarting the webserver will clear all locks.

Once you have clicked on the Radio Button and entered the necessary information, click on the Release Locks button.
Note: Validation is not performed on the User Id(s) or IP Addresses entered.

Reports

The Reports section contains information about auditing, viewing attachment status, diagnostics, and server statistics.

Topics

- *Audits*
- *Alert History*
- *Attachments*
- *Diagnostics*
- *Statistics*

Audits

Search Audits

The Search Audits section allows you to search through all the audit logs that have been generated for each transfer done using Slingshot.

Navigation: Reports > Audits > Search Audits

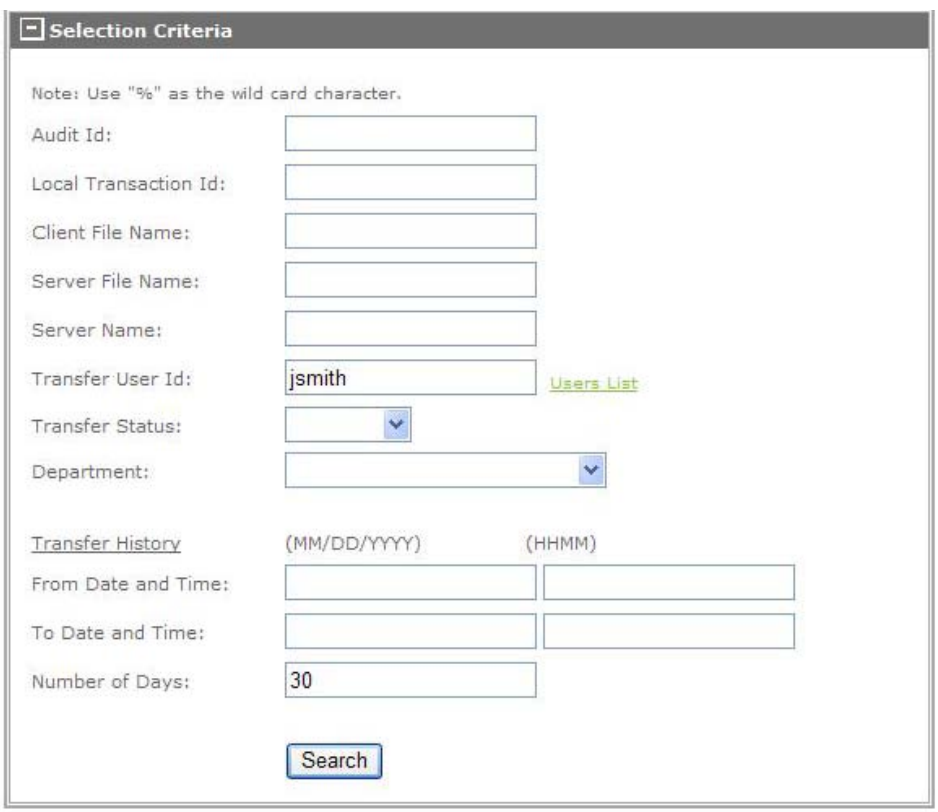


Figure 44

The Search page will hold a list of the first 100 Audit Ids that meet the selection criteria. The Selection Criteria can be based on Transfer History information such as Dates, Times and Number of Days.

Delete Audits

Navigation: Reports > Audits > Delete Audits

A user account with the AdministratorRight assigned to it will have the authority to delete audit records. This is done on the Delete Audits web page. To delete audit records, select a Date or Number of Days as well as the Audit Type, and then click on the Delete button at the bottom of the panel.

Alert History

Search Alerts

Navigation: Reports > Alert History > Search Alerts

The Search Alerts page allows you to search for Alerts that have been generated by completed Slingshot transfers. When you enter the Search Alerts page, by default 100 Alert Audit records are displayed within the Results box. The Selection Criteria box allows you to filter the alerts to limit the number of alerts that are displayed in the results box. For a description of the Search Alerts parameters see the section Add Alert.

Selection Criteria

This box allows you to selectively search the Alerts database to limit the number of records that are displayed. The % character is used as a wildcard character to simplify the search. If a field has no search criteria entered, then no filtering will be done on that field. If multiple fields have search criteria defined, the search criteria must match on all defined fields before a record will be returned. When you have completed the Search Criteria, click on the Search button. The output will be placed in the Results table. Up to 100 Alerts will be displayed at a time within the Results table. If more than 100 entries are returned for a search, you can view the next 100 entries by clicking on List Next 100>. If you click on the Alert Audit Id of an entry in the table, a detail page will be displayed that allows you to update the PGP system key configured if you are authorized.

Delete Alerts

Navigation: Reports > Alert History > Delete Alerts

The Audit Delete page allows you to delete Slingshot records from the Audit database.

There are two options to determine the Audit records to delete:

Delete Audit Records Older Than Month**/Day/Year allows** you to define a date where all Audit Records older than that date will be deleted.

Delete Audit Records Older Than xxx Days allows you to define the number of days of Audit records that you want to save. All Audit records older than those days are deleted.

Every Audit record that is deleted is saved in a file in the Install Audit directory created during the Slingshot installation.

Attachments

The Attachments Search page allows you to search for Slingshot emails and attachments. The Selection Criteria box allows you to filter the search to limit the number of records that are displayed in the results table.

Navigation: Reports > Attachments

Figure 45

Above is an example showing two emails sent with attachments, while this list only shows two items, the page will hold a list of the first 100 attachment records.

By clicking on the link for any of the attachment records contained in the Subject column you will be shown the Slingshot Details of that email attachment record.

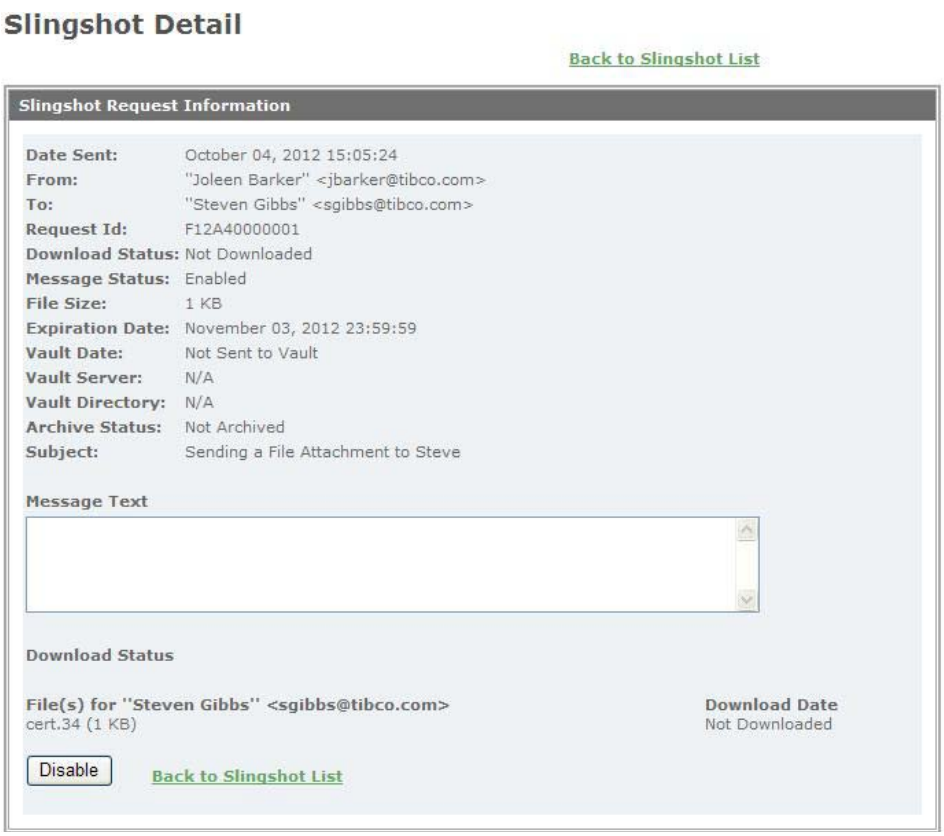


Figure 46

This detail page shows the time of the email, the last file download time and the contents of the email.

Diagnostics

The Diagnostics page displays information for one or more Slingshot servers that may be sharing a database. This information will assist TIBCO Technical Support Team in solving issues with Slingshot.

Navigation: Reports > Diagnostics

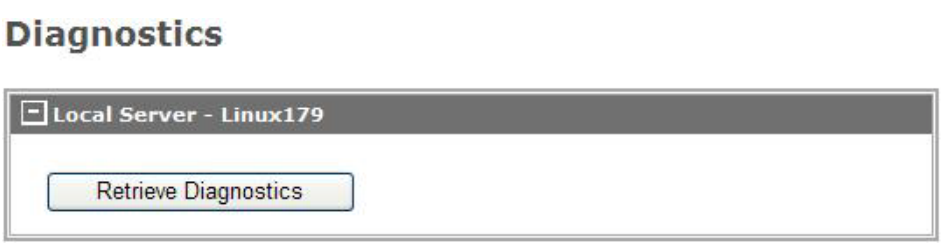


Figure 47

Each server displayed can be expanded to display the Retrieve Diagnostics button. By clicking on the button the details regarding the installation and setup will be displayed. When this information is needed you may be asked to supply a screenshot of the information seen here or to supply a file with the information in it. To create the file simply click on the Save Server Diagnostics to File link to save the information to an html file.

Statistics

Information on the Statistics page includes daily, weekly and monthly transfer byte counts and more.

Navigation: Reports > Statistics

Below is a screenshot of the information you will see listed on this page at this time:

Figure 48

Slingshot Text Field Lengths

Below is a table comprised of the field lengths for all the string fields available on the Slingshot Administrator web pages:

Field (Web Page field is on)	Size
User ID (Add User)	64
Full Name (Add User)	256
Password (Add User)	32
Confirm Password (Add User)	32
Email Address (Add User)	64
Description (Add User)	64
Company Name (Add User)	64
Phone Number (Add User)	64
IP Address or IP Name (Add User)	64
Netmask (Add User)	64
Department Name (Add Department)	64
Description (Add Department)	256
Server Name (Add Server)	64
IP Name (Add Server)	80
IP Port (Add Server)	5
Server File Name Prefix (Add Server)	256
Default User (Add Server)	32
Default Password (Add Server)	32
Confirmed Password (Add Server)	32
Default Windows Domain (Add Server)	256
Description (Add Server)	256
Excluded Word List File Name (System Configuration)	255

Field (Web Page field is on)	Size
Embedded Word List File Name (System Configuration)	255
Minimum Password length(System Configuration)	2
Maximum Password Length(System Configuration)	2
Required Number of Numeric Characters(System Configuration)	2
Required Number of Special Characters(System Configuration)	2
Minimum Number of Unique Characters(System Configuration)	2
Enforce Password History (System Configuration)	2
Maximum Days Between Password Change (System Configuration)	3
Minimum Days Between Password Change(System Configuration)	3
Advance Notice of Expiring Password(System Configuration)	2
Password Reset Expiration (System Configuration)	10
Display Name(System Configuration)	255
Email URL (System Configuration)	255
IP Address (System Configuration)	64
IP Port (System Configuration)	5
Context (System Configuration)	32
Email Recipients When User Adds Key(System Configuration)	256
Email Template(System Configuration)	64
Email Host Name(Slingshot Configuration)	64
Email Host Port (Slingshot Configuration)	5
Email Admin User ID (Slingshot Configuration)	64
Email Admin User Pwd(Slingshot Configuration)	64

Field (Web Page field is on)	Size
Email Sender (Slingshot Configuration)	64
Repository Directory(Slingshot Configuration)	255
Internal Email Domains (Slingshot Configuration)	255
Transfer Size Rules (Slingshot Configuration)	4
Maximum Expiration (Slingshot Configuration)	11
Maximum Number of Recipients (Slingshot Configuration)	11
Maximum File Size Per Email (Slingshot Configuration)	11
Vault Directory(Slingshot Configuration)	255
Retention Period (Slingshot Configuration)	11
Alert Description (Add Alert)	256
Elapsed Time (Add Alert)	9
Client File Name (Add Alert)	256
Server File Name (Add Alert)	256
Transfer User ID (Add Alert)	64
Transfer Description (Add Alert)	256
Template File for additional Criteria (Add Alert)	256
Recipient (Add Alert)	64
Email Template File (Add Alert)	64
Comment (Add Alert)	64
Community Name (Add Alert)	256
Enterprise Object ID(Add Alert)	256
SNMP Server IP(Add Alert)	80
SNMP Agent IP(Add Alert)	80
Specific Trap ID(Add Alert)	5
Message Object ID(Add Alert)	256
Message (Add Alert)	256

Field (Web Page field is on)	Size
Trap Port(Add Alert)	5
Full Path of Command to Execute (Add Alert)	256
Parameters(Add Alert)	256
Full Class Name (Add Alert)	256
Parameters (Add Alert)	256
Enter the PGP Public Key in the box below (Add PGP Public Keys)	2GB
Description (PGP System Keys)	255
Pass Phrase (PGP System Keys)	255
Confirm Pass Phrase (PGP System Keys)	255
Real Name (PGP System Keys)	64
Email Address (PGP System Keys)	64
Private Key Pass Phrase (PGP System Keys)	64
Confirm Pass Phrase (PGP System Keys)	64
Private Key Pass Phrase (Import PGP System Key)	112
Confirm Pass Phrase (Import PGP System Key)	112
Description (Import PGP System Key)	255
Enter the PGP Secret Key in the box below (Import PGP System Key)	2GB
Enter the PGP Public Key in the box below (Import PGP System Key)	2GB
Description (PGP System Keys)	255
Authenticator-UserName (LDAP Sync)	64
Authenticator Name (Add Authenticator)	16
Host Name/ IP Address (Add Authenticator)	80
Bind User DN (Add Authenticator)	255
Bind Password (Add Authenticator)	64

Field (Web Page field is on)	Size
Confirm Password (Add Authenticator)	64
Base DN (Add Authenticator)	255
Full Name (Add Authenticator)	64
Distinguished Name (Add Authenticator)	64
Email Address (Add Authenticator)	64
Alternative Email Address (Add Authenticator)	64
User Name (Add Authenticator)	64
Phone Number (Add Authenticator)	64
Delete Audit Records Older Than (Audits)	3
Delete Alert Records Older Than (Alert History)	5