



Martus™ Server Policy Administration (MSPA) Tool

User Guide

Version 1.0 (December 2007)

© Copyright 2001-2007, Beneficent Technology, Inc. (Benetech), Palo Alto, California. Nongovernmental organizations (NGO's) may freely copy and distribute this manual, but may not sell or distribute it for commercial purposes.

The copyrighted Martus™ software itself was developed with funding from several organizations, foundations, and The Benetech Initiative itself. To obtain more information, visit the Martus Project website at <http://www.martus.org>.

The Martus software has been developed and is being distributed under a free/open source license. To learn more and to understand the terms of use, please visit <http://www.martus.org/license.html>. Martus is a trademark and service mark owned by Beneficent Technology, Inc., formal registration of which is pending in the United States and elsewhere. Please acknowledge this mark by use of the ™ symbol with it, when first referring to it in other documentation. For simplicity, we have not used the ™ symbol in this documentation and often refer only to “Martus” when referring to the software and the program, except on the introductory pages. Benetech claims world-wide ownership of the Martus mark for this particular set of uses and services.

Table of Contents

1. Introduction	4
2. Setting Policies for Martus Servers	4
2a. Identifying a Server	4
2b. Granting and Denying Upload Rights to Client Accounts	4
2c. Managing Accounts and Bulletins.....	4
2d. Policy Administrator Tasks.....	5
2e. Mirroring Records	5
2f. Choosing a Strong Passphrase	5
3. Setting up the MSPA Client	6
3a. Installing the MSPA Client	6
3b. Creating your account	6
3c. Exporting your Account's Public Key	8
3d. Setting up a Server connection.....	9
4. Using the MSPA Tool	11
4a. Monitoring and modifying accounts	11
4b. Server compliance statement.....	13
4c. Managing Magic Words	14
4d. Backing up servers	14
4e. Starting and stopping the Martus Server service.....	16
4f. Identifying the version of your MSPA Tool	17
Frequently Asked Questions.....	18
Appendix A. Configuring a Compliant MSPA Workstation.....	19
Appendix B. MSSA instructions for setting up the MSPA Client and Server	20

1. Introduction

Each Martus™ Backup Server must have a Policy Administrator, who sets and enforces the policies that determine how the server can be used. A Martus Server Policy Administrator (MSPA) does not need technical skills or knowledge. However, to make appropriate policy decisions, you need to understand the features of the Martus Server. This guide describes the general features and policy decisions that you, as the MSPA, control, using the Martus Server Policy Administration (MSPA) Tool. In some cases, you will need to request that the technical System Administrator actually make the policy changes for you, and the System Administrator will report back to you.

The first section of this manual provides information about setting policy for Martus Servers; the second section documents the Martus Server Policy Administration (MSPA) Tool.

2. Setting Policies for Martus Servers

2a. Identifying a Server

Each Martus Server is accessed through an IP address, such as 10.121.205.11. The technical System Administrator will choose the IP address, and provide that information to the MSPA. Each server also has a unique "Public Code," which is automatically created when the server is initially configured. A Public Code comprises twenty digits, written as five groups of four digits. For example, a Public Code might be 1234.5678.2345.6783.4567. Martus Clients use a combination of the server's IP Address and Public Code to identify a specific server. If either of these values changes, all the existing clients need to be notified.

2b. Granting and Denying Upload Rights to Client Accounts

Martus Servers keep track of which Martus Clients are allowed to upload bulletins. Once a particular client obtains upload rights, that client will have full use of the server indefinitely, unless you choose to disallow uploads for that account, or to completely "block" that client (which disallows both uploads and retrieval of previously created bulletins from the server). As with servers, you'll identify client accounts by their Public Codes.

Rather than requiring you to grant upload rights individually for client accounts, Martus Servers rely on *Magic Words*, which are specific to a particular server. A Magic Word is a word or phrase that a new client enters once in order to request upload rights on a server. Typically, the organization that sets up a new Martus Client provides the client with the information they'll need to begin uploading bulletins to a Martus Server: the server's IP address, Public Code, and a Magic Word. As you distribute Magic Words to Martus Client users, inform them if you plan to deactivate the Magic Word at a certain date.

Theoretically, you could create a different Magic Word for each client. However, in practice, server operators tend to use a single Magic Word for each group of clients (for example, one Magic Word for each project, training session or Headquarters). You can add and remove Magic Words, and view a list of currently active Magic Words.

2c. Managing Accounts and Bulletins

You can choose to block (or "ban") an account, perhaps because that account is using the server for illegitimate purposes. When you block an account, all the bulletins associated with it remain on the server, but a banned account cannot retrieve or augment old bulletins, or upload new bulletins unless the account is unblocked. However, any (unblocked) HQ accounts associated with a banned account could still retrieve the bulletins. At any time, you can view the status of client accounts to see whether they have upload rights or have been blocked. You can view the bulletins on the server for any client account, or view any available contact information for a given account. You can "hide" a bulletin, which will make it impossible for users to retrieve (you can recover it, and the system administrator can access it); you should only do this in accordance with the Server Compliance Statement in effect on this server at the time.

2d. Policy Administrator Tasks

As a Martus Server Policy Administrator, you can perform several tasks related to server policies. During initial configuration, the server creates both a Public Key and a Private Key. Together, the Public Key and Private Key are referred to as the key pair. To use the MSPA Tool, you'll need to have your own key pair (different from the server), and you'll have to submit your Public Key file to the technical System Administrator, who will grant you access. All policy administrative actions are logged. The technical System Administrator can see which tasks were done, by whom, and when. This is an important security feature, to help the System Administrator detect whether an unauthorized person is modifying the server.

2e. Mirroring Records

You can mirror, or back up, the records on your server so that they are copied to another server. Likewise, you can mirror other servers' records. Benetech encourages you to mirror records to any server that is Compliant and whose administrator is willing to back up your records. In turn, if you have the capacity and the resources, we encourage you to be willing to be back up other servers' records.

2f. Choosing a Strong Passphrase

One way to create a good passphrase (or password) is to use one of the high-quality passphrases that the Martus server software creates for the Martus Server System Administrator when they set up the server key pair.

Alternatively, you can create a passphrase that includes several digits and punctuation characters, and is at least twenty characters long. Passphrases should never contain names of family members, friends, pets, towns, cities, or countries. They should not contain made-up words from movies or books. Do not use the first letter of each word of a sentence, unless the sentence is unusual, and you thought up the sentence yourself, and you keep the sentence secret.

A passphrase should not contain any dates, phone numbers, or street addresses. It should not contain any words that can be found in any dictionary of any language (unless you use the diceware method mentioned above). Do not use dictionary words with letters replaced by digits, like "p01nt".

MSPAs might only use the passphrase on a weekly or monthly basis, so it will be difficult to remember it between uses. In an environment that is physically secure, and where you protect the written copy very carefully, it is safest to use a passphrase that is so complex that even you can't remember it without referring to a written copy. Even if you choose a passphrase that you can remember, you should always keep a written copy safely locked away in a very secure location, in case you forget it.

Except when you are using the passphrase, don't keep a written copy of it on your person, anywhere near your desk, or near the server. This applies even if the written copy is a "coded" version of the real passphrase that reminds you of the real passphrase. Also, please be aware that someone might try to steal your passphrase by watching over your shoulder as you type.

Attackers can be surprisingly clever. Also, remember that anyone who wants to steal your passphrase has probably read this advice.

In this release, the MSPA client has no feature right now to change passwords. This may be available in future releases, but see the FAQ #7 for instructions on what to do if you forget your password in this release.

3. Setting up the MSPA Client

3a. Installing the MSPA Client

These tasks will most likely be performed by the Martus Server System Administrator (MSSA).

Before installing the MSPA Client, you must have configured a compliant MSPA Workstation. See Appendix A for instructions on how to do this.

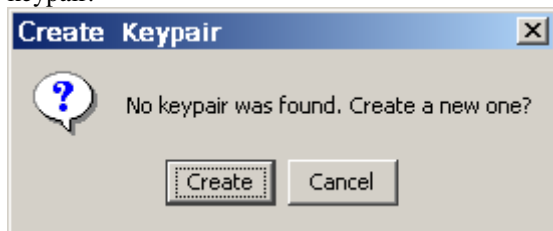
The steps below describe setup for the MSPA Client. Please See Appendix B for MSSA instructions on steps required to complete setup on the MSPA server side.

To install the MSPA Client:

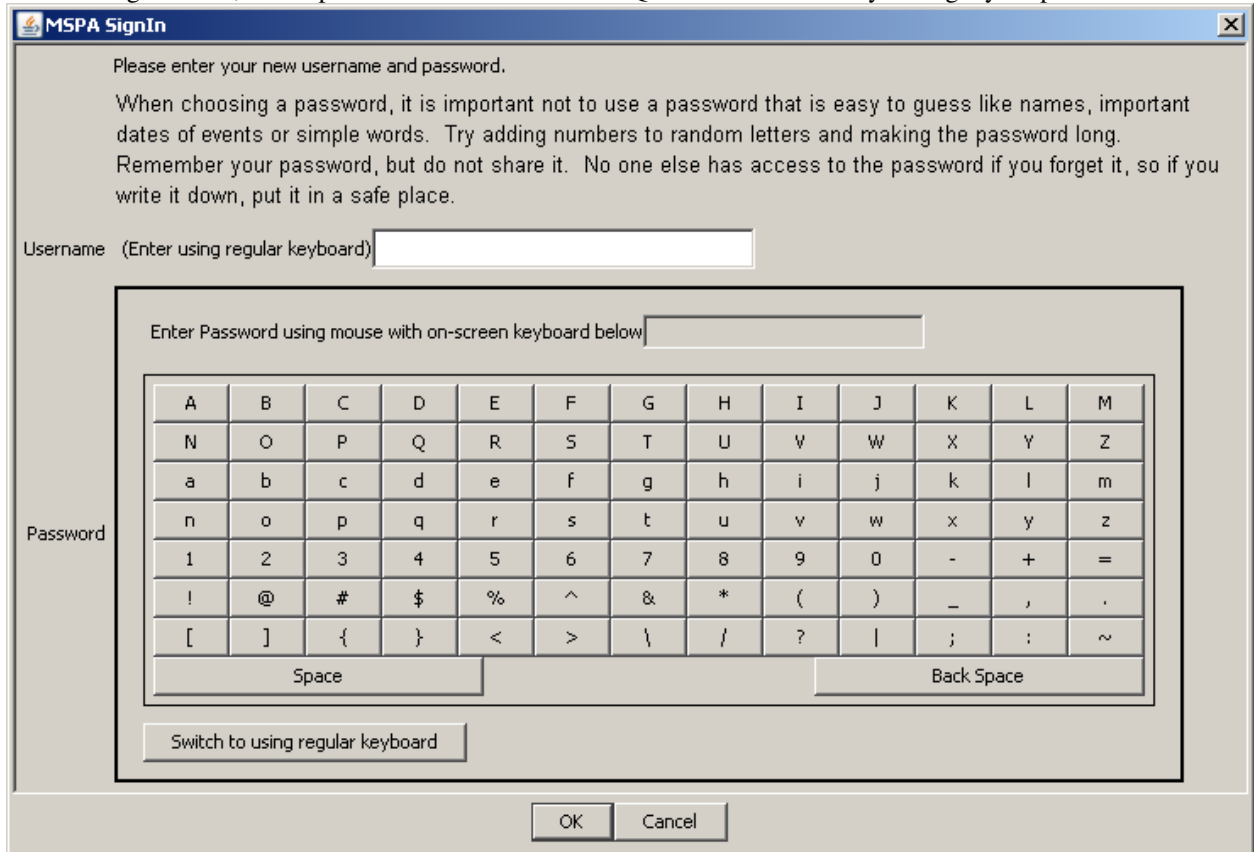
1. Unzip MSPA.zip in C:\ in Windows, or in the directory of your choice for Mac/Linux. The zip file contains program files, shortcut to run MSPA tool for Windows, MSPA Client User Guide (this document)
2. Download and install Java 1.6. You can confirm that it is properly installed by typing this command at a command line prompt:
java -version
3. For Windows, Java should be installed in C:\Program Files\Java. For Mac/Linux, determine where your default Java is installed by typing this command at a command line prompt:
For Mac: type java
For Linux: echo \$JAVA_HOME
4. Download and install the Sun crypto policy files from <http://java.sun.com/javase/downloads/?intcmp=1281>. At the bottom of the page, click on the Download button for "Other Downloads" (that mentions "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6"). Unzip the downloaded file (which contains a directory with US_export_policy.jar and local_policy.jar inside it) and copy those jar files to the lib\security folder within your Java install (e.g. C:\Program Files\Java\jre1.6\lib\security in Windows, \$JAVA_HOME/lib/security/ in Linux), replacing any files with the same name.
5. Copy the bcprov file in the ThirdParty directory to the lib\ext folder within your Java install (e.g. C:\Program Files\Java\jre1.6\lib\ext in Windows, \$JAVA_HOME/lib/ext/ in Linux)
6. Copy the MSPA shortcut to your desktop if desired (for Windows).
The MSPA can also be run from the command line using the following command:
Windows: java -jar C:\MSPAClient\martus-mspa-client.jar
Mac/Linux: java -jar directory-where-you-unzipped/MSPAClient/martus-mspa-client.jar

3b. Creating your account

1. Start the MSPA Client by double-clicking the shortcut (either on your Desktop or in the MSPA install directory.)
2. If this is the first time you use the MSPA Client, the application will guide you through the creation of your keypair.



3. Create a username; it can contain letters, numbers, punctuation, and spaces. We recommend that you create a username that has between 8 and 50 characters, and recommend against entering non-ascii characters using the Alt + NumberPad method. Choose a username that will be easy for you to remember, and remember how you capitalize it, as MSPA usernames are case-sensitive.
4. Click characters on the on-screen keyboard to type a password that has between 8 and 50 characters. (There is no cursor in the Password field, and you do not have to click in it.) Choose a password that you can remember, but that would be difficult for someone else to guess. Use a combination of letters, numbers, and punctuation to make the password more secure. See “Choosing a Strong Passphrase” for guidelines for creating a secure, useful password. Please see the FAQ #7 for what to do if you forget your password.



MSPA SignIn

Please enter your new username and password.

When choosing a password, it is important not to use a password that is easy to guess like names, important dates of events or simple words. Try adding numbers to random letters and making the password long. Remember your password, but do not share it. No one else has access to the password if you forget it, so if you write it down, put it in a safe place.

Username (Enter using regular keyboard)

Enter Password using mouse with on-screen keyboard below

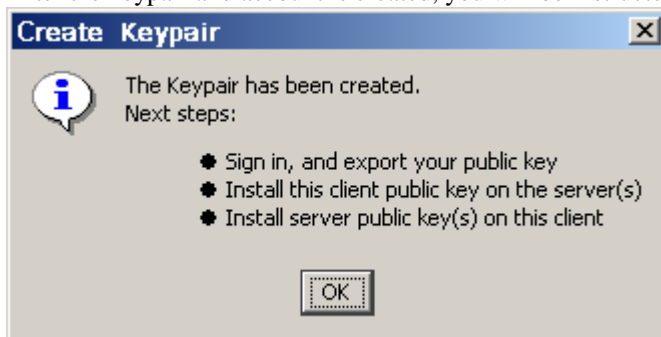
A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	b	c	d	e	f	g	h	i	j	k	l	m
n	o	p	q	r	s	t	u	v	w	x	y	z
1	2	3	4	5	6	7	8	9	0	-	+	=
!	@	#	\$	%	^	&	*	()	_	,	.
[]	{	}	<	>	\	/	?		;	:	~
Space						Back Space						

Switch to using regular keyboard


OK Cancel

Note: If you prefer to type your password using the computer’s keyboard, click Switch To Using Regular Keyboard. Your password may be less secure if you type it with the computer’s keyboard than if you use the on-screen keyboard, as an unauthorized person could install a device or program that could “sniff” your keyboard to record your keystrokes. If using the keyboard, we recommend against entering non-ascii characters using the Alt + NumberPad method.

5. Click OK.
6. After the keypair and account is created, you will be instructed to sign in and export your public key.



Create Keypair

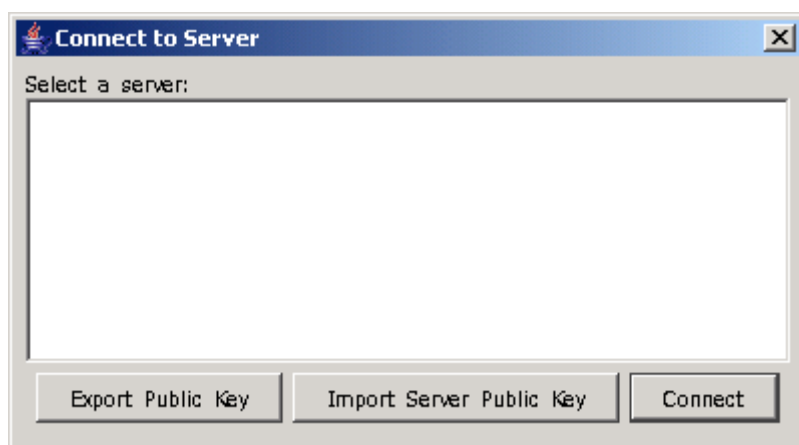
 The Keypair has been created.
Next steps:

- Sign in, and export your public key
- Install this client public key on the server(s)
- Install server public key(s) on this client

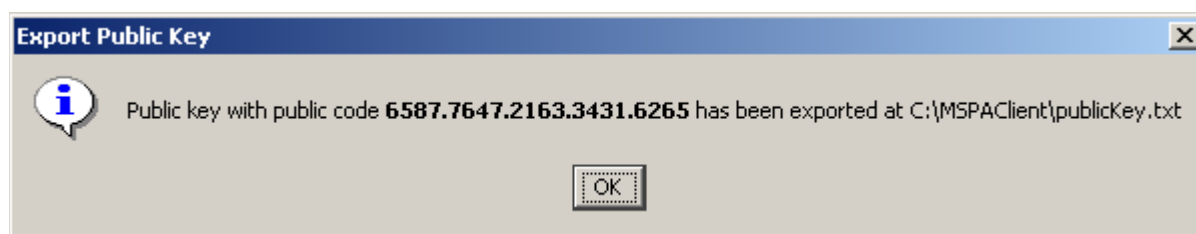
OK

3c. Exporting your Account's Public Key

Before you can access Martus servers using the MSPA Tool, you must export your Public Key and give it to the Martus server system administrator. To export the Public Key, click the "Export Public Key" button in the initial MSPA screen.



Then click OK in the confirmation dialog box.

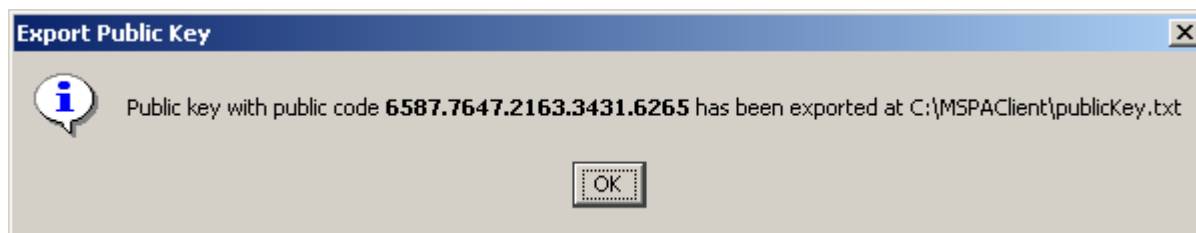
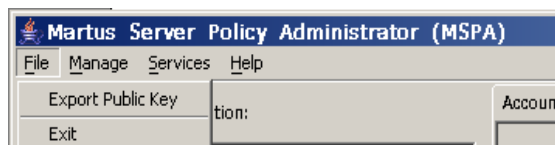


Note the public code generated for the keypair.

Once you have successfully exported the public key, send it to your Martus Server System Administrator for installation on the server. You also need to provide your machine's IP address and the public code.

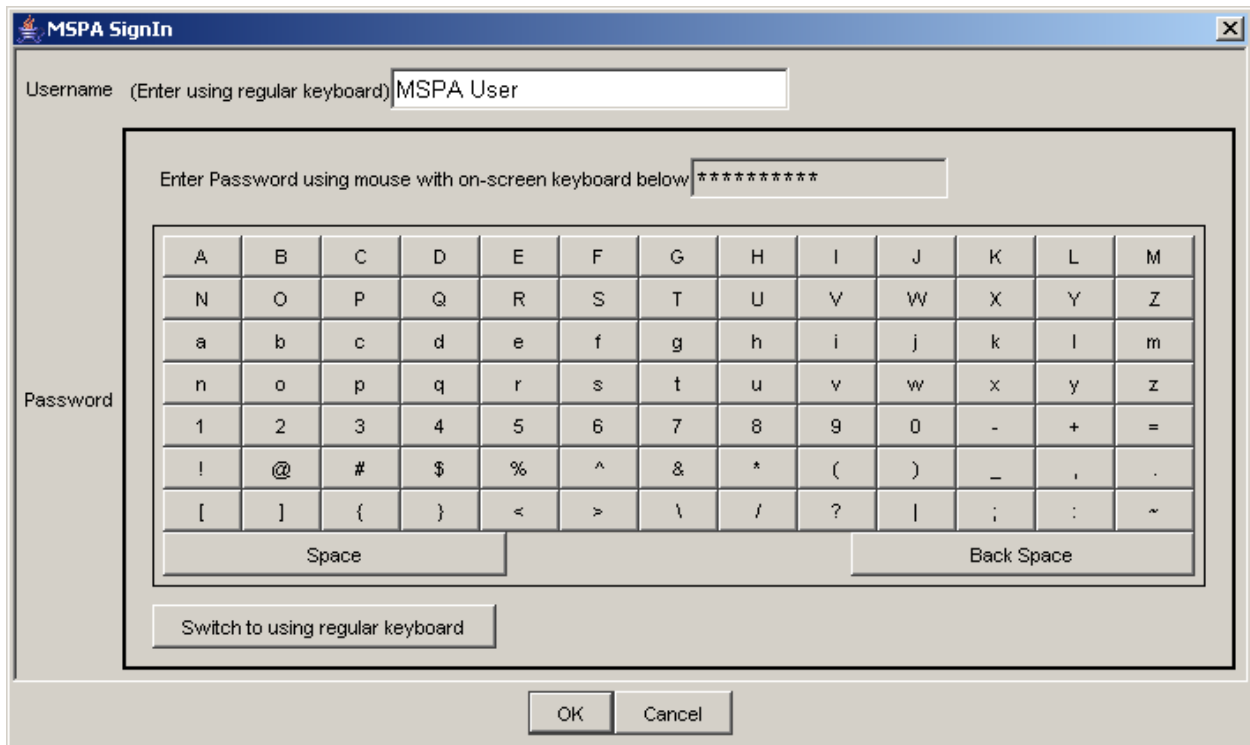
When the client public key is installed on the server, you can now use the MSPA client to connect to the server.

If you need to export your public key again at a later point, you can choose File > Export Public Key. Then click OK in the confirmation dialog box.

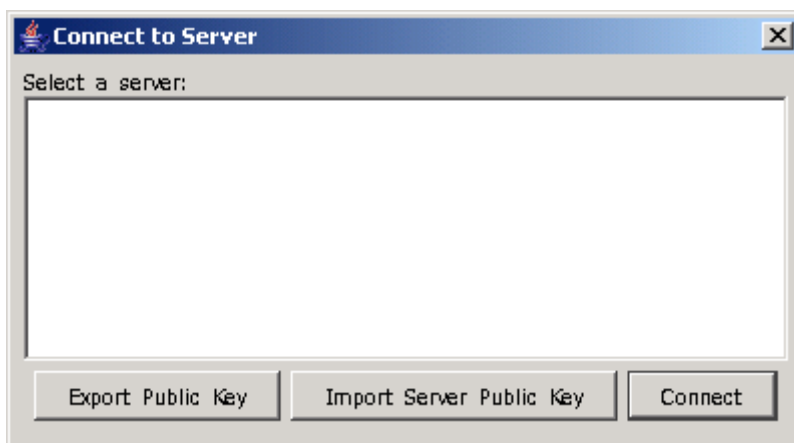


3d. Setting up a Server connection

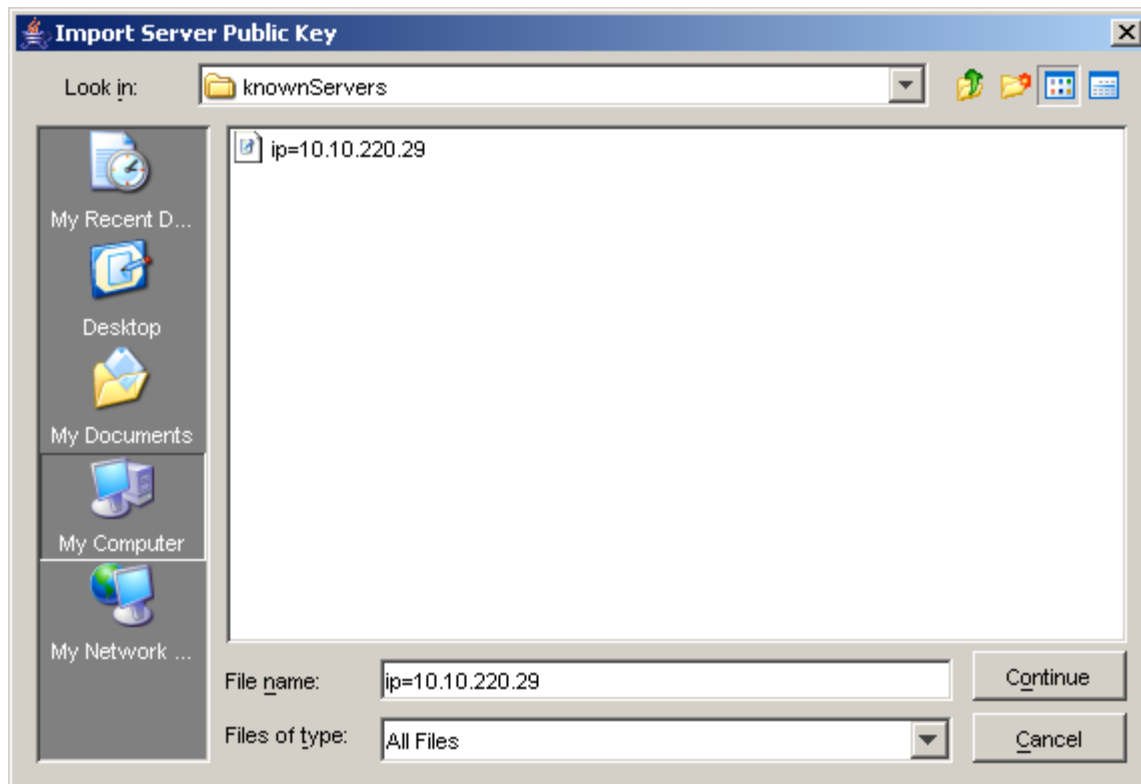
When you start the MSPA Tool, the MSPA Signin dialog appears. Enter your username and passphrase to log on to the server. Then click OK.



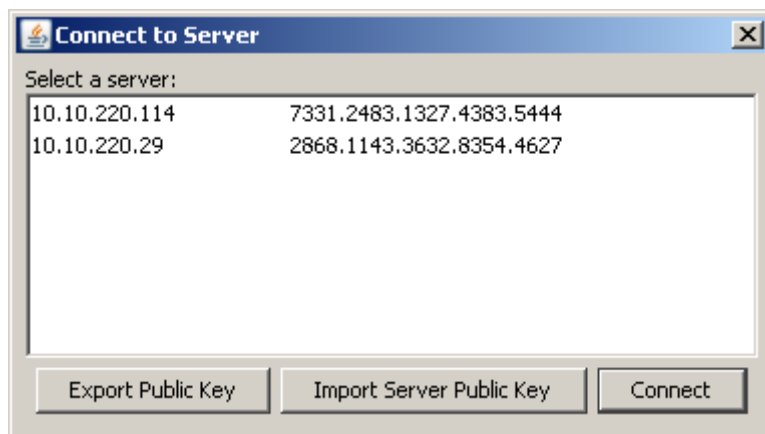
If you have not yet imported the public key of the server you want to connect to, do so now by clicking “Import Server Public Key”.



You will be prompted to find the server public key file given to you by your Martus Server System Administrator (the filename will include the IP address, such as "ip=1.2.3.4").



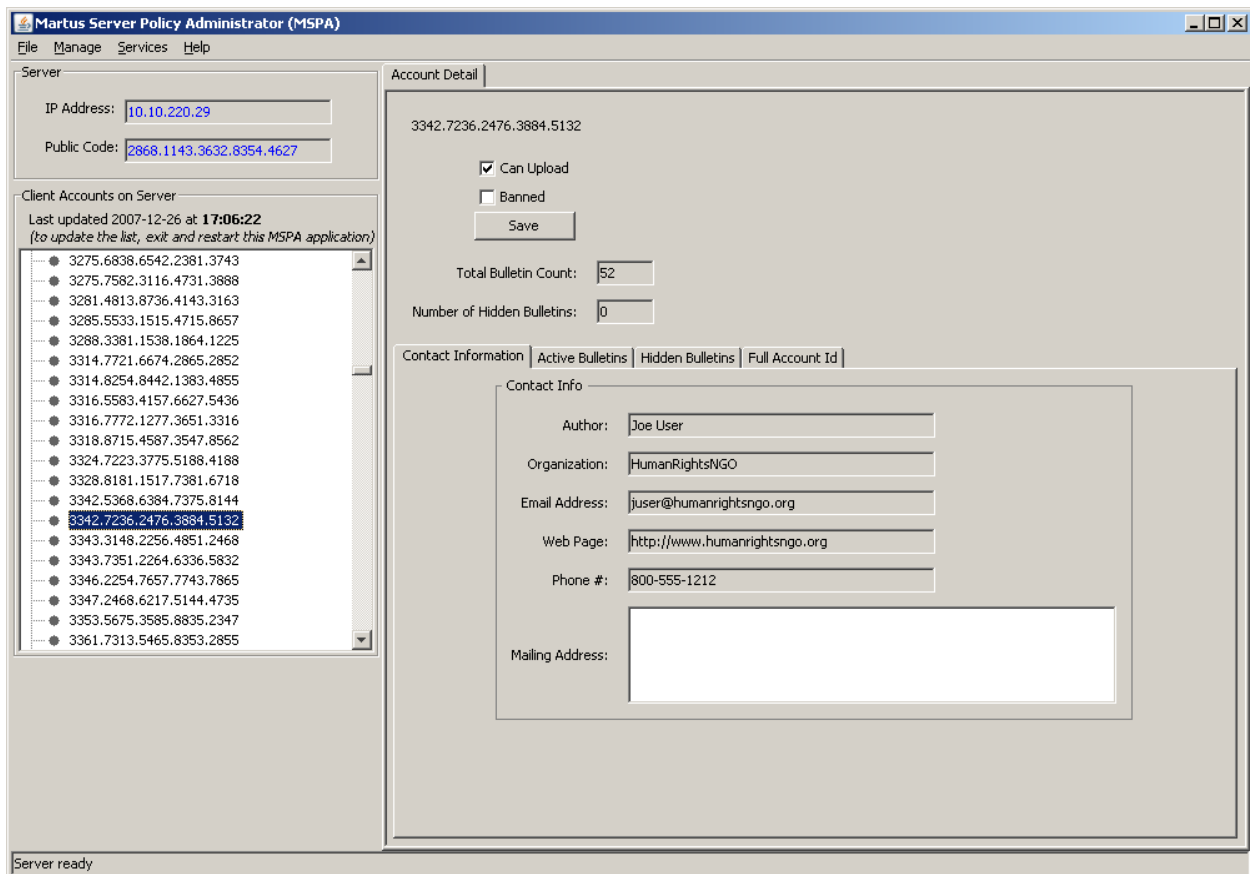
The Connect to Server dialog box appears. This dialog box lists the IP addresses and Public Codes for the Martus Servers you can access. Select a server, and then click Connect.



4. Using the MSPA Tool

4a. Monitoring and modifying accounts

After you connect to the server, you'll see the Account Information screen, which displays details about the Martus Client accounts on the selected server. You can make changes to the status of an account or a particular bulletin. Click Save to submit those changes to the MSPA server.



The Account Information screen displays the following information:

IP Address and Public Code: The MSPA server's IP address and Public Code are displayed in the MSPA Server Information section of the window. Provide this information to Martus Client users, along with a Magic Word. The server's Public Code is actually a short version of the server's Public Key.

Martus Client accounts: On the left side of the window is a sorted list of the Public Codes for the Martus Client accounts on the server. The account list is only updated as of time you started the MSPA Client. Select an account, by clicking on its public code, to view information about it or to change its status.

Details about Martus Client accounts

When you select an account, its information is displayed on the right side of the screen.

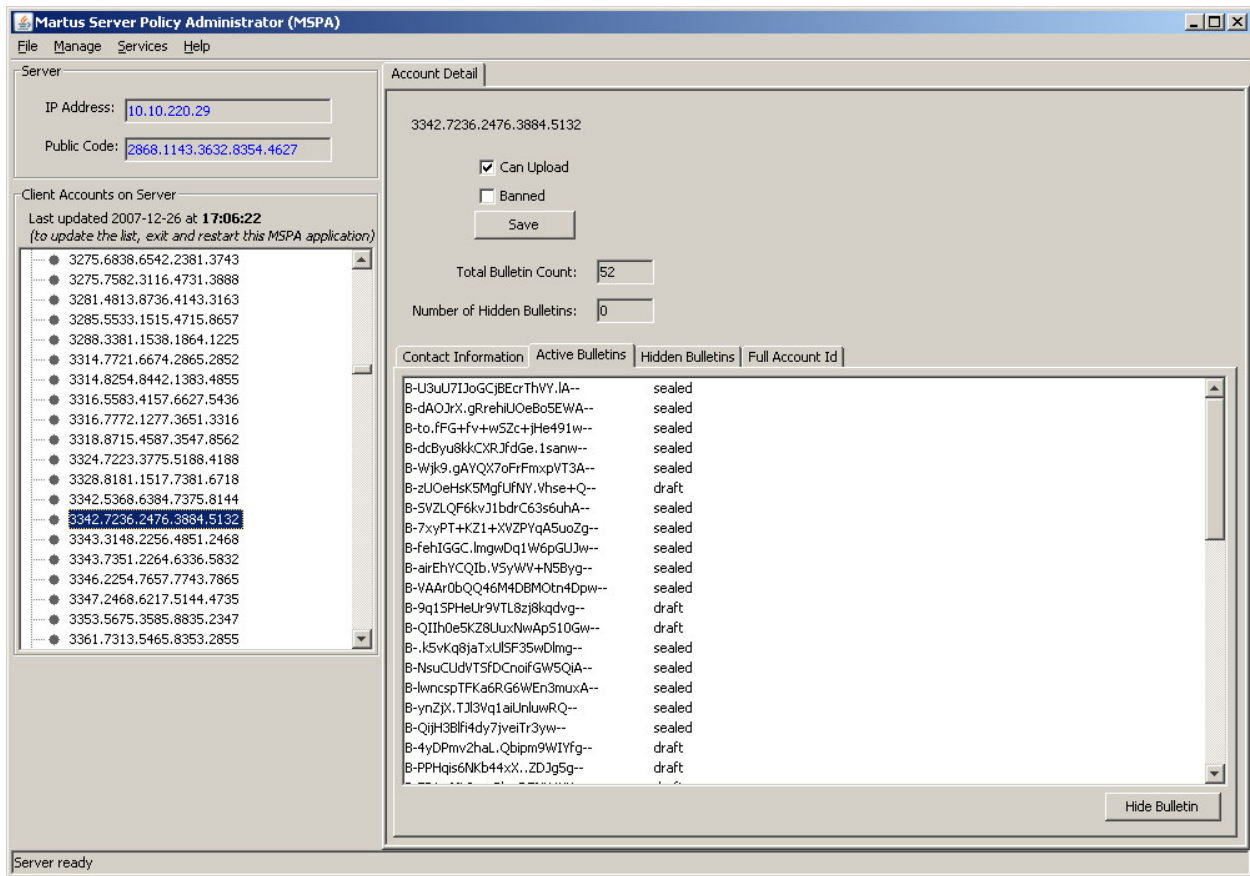
Contact Information: The contact information for the selected Martus Client account is displayed in the center of the window. This information is available if the account owner has chosen to upload it to the server.

Account Status:

- When Can Upload is checked, the account can upload bulletins to the server. Can Upload is checked when an account has submitted a valid Magic Word.
- When Banned is checked, the account cannot upload or retrieve any bulletins. To restore an account's privileges, uncheck Banned. Banned status overrides any other checkboxes on the screen.

Active Bulletins: Each active bulletin for the account is listed, with its status (draft or sealed). You can hide a bulletin, which prevents anyone (the Martus Client account that created it, or any HQs associated with that account) from retrieving it from the server; you should hide a bulletin only in accordance with the Server Compliance Statement in effect on that server. A hidden bulletin is not physically removed from the server; a system administrator can retrieve it, and you can recover it in the Hidden Bulletins tab. To hide a bulletin, select it and click Hide Bulletin.

Hidden Bulletins: The number of hidden bulletins for the selected account is listed in the Account Detail section. To see which bulletins were hidden, click the Hidden Bulletins tab in the lower section of the window. To recover a hidden bulletin, select the bulletin and click Recover Hidden Bulletin.



Note: To work with a client account, you must know its Public Code, which the account user can view by choosing Help > View My Account Details in the Martus Client. Many server logs of client activity also display the Public Code, but it's difficult to identify users based on server log activity, so it is not a reliable way to determine the Public Code for a user.

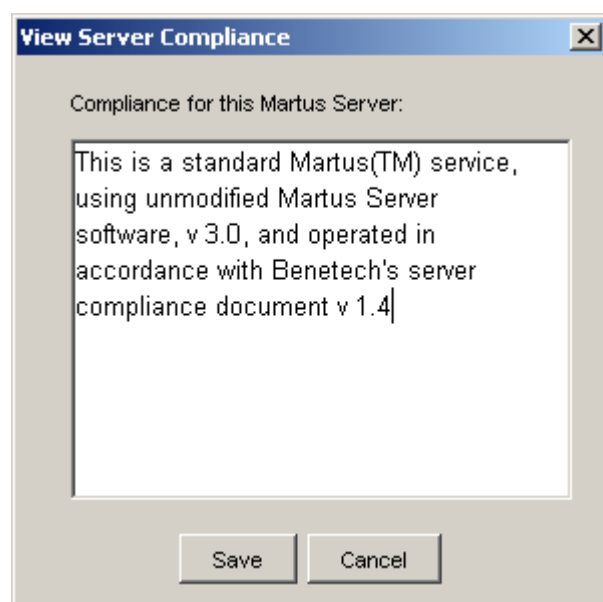
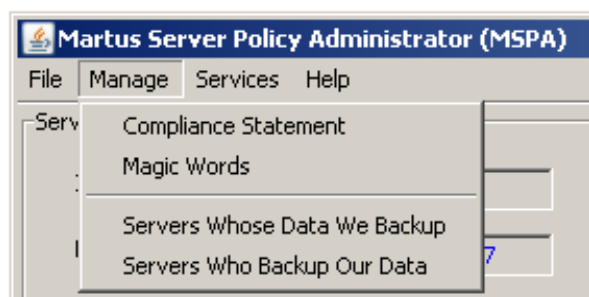
Any changes you make to Account settings will require a restart of the Martus service before they take effect. See “4e. Starting and stopping the Martus Server service” for more information.

While you may be able to locate an account by scrolling through list to see the contact information that the clients have chosen to upload, we do not recommend using contact information to specify the account, because the contact information may be incorrect, or multiple accounts may have similar or even identical contact information.

Enhancements in future versions of the MSPA Client may allow you to search for contact information or a public code (if you do not know the beginning or entire public code to find it on the list) and provide a list of banned accounts – until these are available in the Client tool, your MSSA may be able to do this for you by logging onto the server-side command line version of the MSPA. Future releases may also include various reports about server activity and usage, and the ability to designate whether an account’s bulletins can be “amplified” to a web-based Martus Search Engine.

4b. Server compliance statement

A Compliant server is a carefully managed Martus Server where Benetech's security and service recommendations are followed. To review or edit a server’s compliance statement based on the Martus requirements, choose Manage > Compliance Statement. Please see the Martus Server Compliance Guidelines (available with the Martus Server software) for more information on requirements for maintaining a compliant server. The specific wording of the compliance statement should not be changed from the designated text displayed below, except as described in the Martus Server Compliance Guidelines and FAQ.



Any changes you make to the Compliance statement will require a restart of the Martus service before they take effect. See “4e. Starting and stopping the Martus Server service” for more information.

4c. Managing Magic Words

The Magic Word is a code word that a Martus Client user must enter to gain initial access to a Martus Server. It need only be entered correctly once; from that point on, the account has access to the server unless you ban it or the server is stopped or otherwise unavailable.

To see the Magic Words currently in effect, their status, and their group assignment—or to add, update, activate, or deactivate magic words, choose **Manage > Magic Words**. Each current Magic Word is listed in the Magic Words dialog box, along with its creation date, status, and group assignment.

To activate a Magic Word, check the active box in the Status field. To deactivate a Magic Word, uncheck the active box.

Note: Magic Words cannot be deleted, but they can be deactivated.

To add a new Magic Word, type the word, choose a group assignment, and then click **Add**.

To update the group assignment for an existing magic word, select the magic word and either type in a new group or choose one from the dropdown menu, and then click **Update**. You may want to create sets of magic words before you have users to assign them to, and set placeholder group names initially, which you update with a more meaningful description when you actually distribute them to a user or project.

Note: Deactivating a Magic Word does not affect existing Martus Client accounts who have already connected to the server using a Magic Word. Martus Client accounts only need to know the new Magic Word when they connect to a server for the first time. So, deactivating a Magic Word will only stop Martus Client accounts who have not already connected to the server from doing so.

Creation Date	Status	MagicWord	Group
2005-09-12	<input checked="" type="checkbox"/> active	smile 212	Placeholder 72
2005-09-12	<input checked="" type="checkbox"/> active	78 stamp	Placeholder 71
2005-09-12	<input checked="" type="checkbox"/> active	maroon 90	Placeholder 70
2005-09-12	<input type="checkbox"/> active	711 swing	Placeholder 69
2005-09-12	<input checked="" type="checkbox"/> active	task 43	Placeholder 68
2005-09-12	<input type="checkbox"/> active	round 35	Placeholder 67
2005-09-12	<input checked="" type="checkbox"/> active	54 ticket	Placeholder 66
2005-09-12	<input checked="" type="checkbox"/> active	beyond 88	Placeholder 65

In future versions, you may be able to sort the columns in this screen to find magic words more easily.

Any changes you make in the Magic Words screen will require a restart of the Martus service before they take effect. See “4e. Starting and stopping the Martus Server service” for more information.

4d. Backing up servers

You can back up, or “mirror”, data from another server, and you can back up data from your server on another server. To perform these tasks, go to the **Manage** menu, and then choose the appropriate command.

To back up the data from another server, or to have one back up the data from yours, you need to know the remote server’s Public Code and IP address. You can create a name for the remote server’s IP address to make it easier for

you to identify the server; the name doesn't need to be a domain name, and it only needs to be unique on your own server. The Server Name cannot be left blank, should not contain spaces or punctuation, and cannot start with a number. We suggest using lowercase alphanumeric values for the server name.

To add a remote server for mirroring, that server must be running the Martus Server software when you click Add. The remote server will also need to add your server through their MSPA tool before it can back up any data. Once each server has added the other for mirroring, each server will periodically call the other server (at least every hour) to ensure that the local server has a copy of every bulletin on the remote server.

Once the server appears in the Available Servers list, select it and click the ">>" button to move it to the list of servers that are backed up.

To remove a server, select it on the right side of the dialog box, and then click the "<<" button. The server moves to the list of available servers, but is no longer called by your own server, or is no longer authorized to call your server, depending on which dialog you are in. Note that all bulletins that were copied before you remove a mirror server will remain on that server.

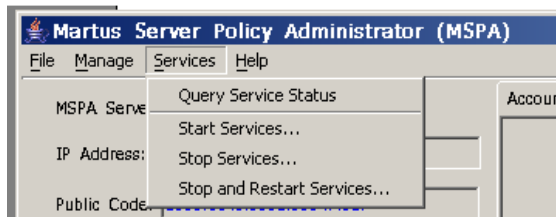
The dialog box is titled "Other Servers: Servers Whose Data We Backup". It contains three input fields: "IP Address:" with the value "10.10.220.41", "Public Code:" with the value "8562.3487.1567.8734", and "Server Name:" with the value "testserver". An "Add" button is to the right of the Server Name field. Below these fields are two lists. The "Available Servers:" list on the left contains one entry: "ip=10.10.220.148-code=5746.2474.7141.3453.3427.txt". The "Servers Whose Data We Backup:" list on the right contains one entry: "ip=10.10.220.151-code=1234.5678.9012.2345.5555.txt". Between the two lists are two buttons: ">>" and "<<". At the bottom are "Save" and "Cancel" buttons.

The dialog box is titled "Other Servers: Servers Who Backup Our Data". It contains three empty input fields: "IP Address:", "Public Code:", and "Server Name:". An "Add" button is to the right of the Server Name field. Below these fields are two lists. The "Available Servers:" list on the left contains two entries: "ip=10.10.220.148-code=5746.2474.7141.3453.3427.txt" and "ip=10.10.220.151-code=1234.5678.9012.2345.5555.txt". The "Can Backup Our Data" list on the right is empty. Between the two lists are two buttons: ">>" and "<<". At the bottom are "Save" and "Cancel" buttons.

Any changes you make to server mirroring/backup settings will require a restart of the Martus service before they take effect. See “4e. Starting and stopping the Martus Server service” for more information.

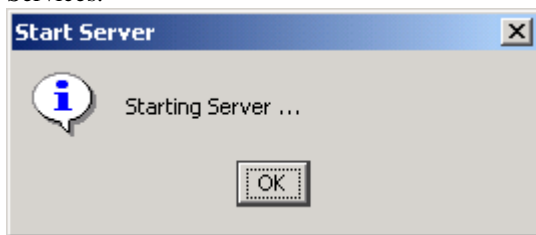
In future versions, you may be able to also similarly designate other servers for amplification – allowing your server’s public bulletins to be displayed on another server’s web-based Martus Search Engine, or allowing another server’s public bulletins to be displayed on your Search Engine.

4e. Starting and stopping the Martus Server service

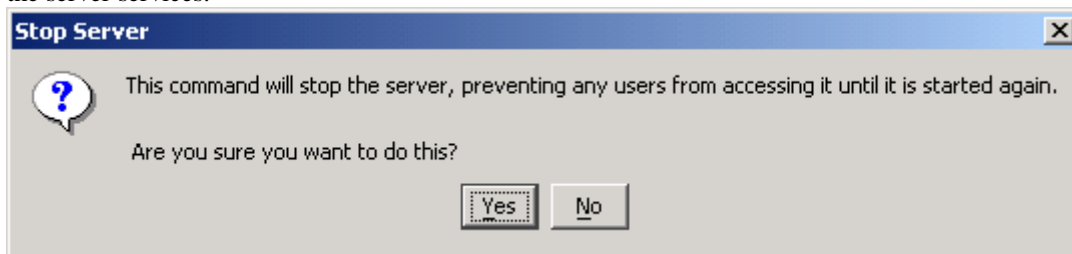


You can check on the status of the Martus Server service by choosing Services > Query Service Status. You can also see it in the status bar in the lower left corner of the MSPA tool screen.

To start the Martus Server service, which enables the backup server software to run, choose Services > Start Services.

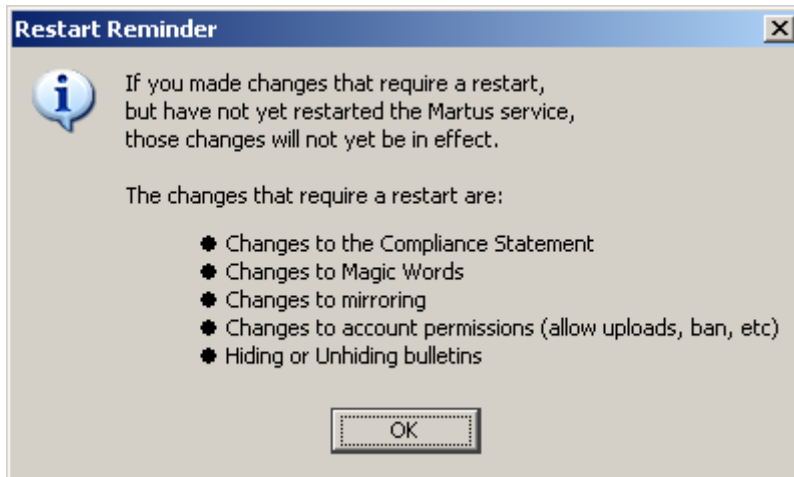
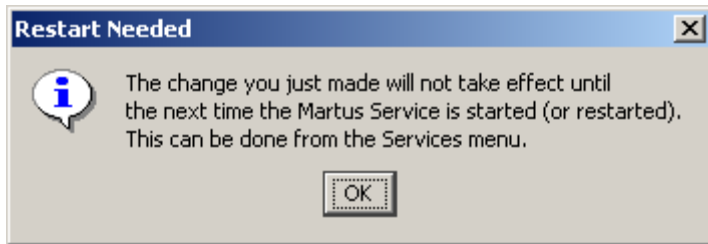


To stop the Martus Server service, choose Services > Stop Services. When you stop the Martus service, no users can access the server until it is started again. Click Yes in the Stop Server dialog box to confirm that you want to stop the server services.



Note: Choosing Start Services or Stop Services enables or disables the Martus Server software, but does not actually turn the physical server on or off.

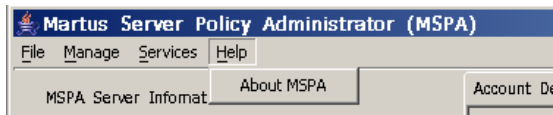
Most of the changes you make while in the MSPA tool will require a restart of the Martus Server service before they take effect. You will be reminded of this when you save any changes, and before you exit.



To stop and restart the Martus Server service (e.g. when settings have changed), choose Services > Stop and Restart Services.

4f. Identifying the version of your MSPA Tool

To see which version of the Martus Server Policy Administrator Tool you're running, choose Help > About MSPA.



Frequently Asked Questions

- 1) What do I do if need help or have questions about running the MSPA tool?
For assistance with running the MSPA tool, please contact help@martus.org.
- 2) Why does the MSPA use IP addresses instead of domain names?
For security. It is easier to spoof a DNS domain name entry than a raw IP address.
- 3) I am getting an "Unable to start MSPA" error. What can I do to fix this?
This may be a result of an incorrect installation. It may due to
 - invalid crypto policy files. If this is the case, you should see the following in the console log: `MartusCrypto$InvalidKeyPairFileVersionException`. For instructions on correctly installing the policy files, see section "3a. Installing the MSPA Client".
 - missing bcprov file. If this is the case, you should see the following in the console log: `org/bouncycastle/jce/provider/BouncyCasteProvider`. For instructions on correctly installing the bcprov file, see section "3a. Installing the MSPA Client".
 - the wrong version of Java is installed. If this is the case, you will see the following in the console log: `ExceptionInInitializer Error`, and `"InvalidKeyException: Public key presented not for certificate signature"`. For instructions on correctly installing Java, see section "3a. Installing the MSPA Client".If you need additional help, please email help@martus.org.
- 4) Can I use my existing Martus Client keypair for the MSPA client?
No. If you do this you will get an error message.
- 5) Can I use an existing Martus Server keypair for the MSPA client?
No. If you do this you will get an error message.
- 6) How do I change my password?
That is not supported in this version. If you need to change it, you will need to delete your MSPA client keypair and create a new one.
- 7) What if I forget my password?
There is no way to recover it. You will need to delete your MSPA client keypair and create a new one. You will need to re-export it, and have the MSSA install it on the server (and remove the old one).
- 8) Is it better to Restart the service than to Stop it and then Start it?
Yes. A restart is faster, so the service will be down for a shorter time.
- 9) I'm trying to add a new server, but it keeps failing with "No response from server"
That server may be down. Or it might be running but with the backup/mirroring feature disabled.
- 10) Has the MSPA client interface been translated to other languages?
No.
- 11) Can I print reports from the MSPA app?
No. You can take screenshots and print those using other applications.
- 12) How can I remove a server from list of available servers or rename a server?
You will need to ask your MSSA to do this in this release. The MSSA needs to put the server in admin mode, remove the old server keypair file, and then you can add the server with the new name if desired.
- 13) What happens if the Banned and Can Upload checkboxes are both selected at the same time?
The Banned checkbox takes precedence over the Can Upload checkbox, so if both are checked, the account is blocked from uploading bulletins.

Appendix A. Configuring a Compliant MSPA Workstation

This task will most likely be performed by the Martus Server System Administrator (MSSA).

If you're using a firewall on your personal computer and/or your LAN, you'll need to configure the firewall(s) to let your computer initiate an outbound TCP connection to port 984 on the Martus Server. The firewall(s) can prevent all incoming connections.

The requirements for a Compliant remote workstation operating system is any of the three options listed below:

1. Run the operating system directly from a CD-ROM (such as KNOPPIX) with the following specifications:
 - a. No programs or program configuration files may be accessed from any hard disk that is used by a non-compliant operating system; the hard disk can only be accessed to retrieve data needed for MSPA or MSSA operations
2. Use a secured Unix or GNU/Linux workstation with the following specifications:
 - a. The workstation must never boot another Non-Compliant operating system unless any hard disk used by Unix or GNU/Linux is removed (Many operating systems are inherently less secure than GNU/Linux. Running them could compromise the security of the server.)
 - b. The workstation must have a local firewall that
 - accepts no TCP connections
 - only accepts UDP packets on port 53 from a small list of nameservers
 - c. The workstation must not mount any remote filing systems
 - d. The workstation's mail reader must disable HTML rendering, or run as a user with no write permission to any data except its own data
 - e. The workstation's web browser, instant message software, and every other operation must run as a user with no write permission to any data except its own data
 - f. The BIOS must not allow booting from floppy
 - g. The screen must be locked after 15 minutes (or less) of inactivity (e.g., by xscreensaver)
3. Use a single-purpose, secured Microsoft Windows workstation with the following specifications:
 - a. Only the MSPA or MSSA for the associated Martus Server is permitted to use the workstation
 - b. The workstation must never boot another Non-Compliant operating system unless any hard disk used by Microsoft Windows is removed
 - c. The workstation must have a local firewall that
 - accepts no TCP connections
 - only accepts UDP packets on port 53 from a small list of nameservers
 - d. The workstation must not mount any remote filing systems
 - e. The workstation must not use Windows 3.x, 95, 98, 98SE or ME
 - f. The workstation must run with automated notice of new Windows Update patches, and upon notice the MSPA or MSSA must immediately install all new security patches
 - g. From the time the Windows operating system is installed, the workstation must have had no interaction with the local LAN or the Internet, except as necessary for configuration, patching, and SSH access to the Martus Servers; and in particular none of the following may have taken place:
 - Use of an email program to send mail to anyone but an MSSA or MSPA
 - Web browsing, except to download or upgrade Martus-related software, and Windows updates
 - Use of any instant messaging programs
 - h. The BIOS must not allow booting from floppy
 - i. The screen must be locked after no more than 15 minutes of inactivity

Appendix B. MSSA instructions for setting up the MSPA Client and Server

There are three components. Two on the server, and one on the client.

=====

SERVER SIDE

There are two server components: The main MSPA Server, and the RootHelper. If RootHelper is not running, the commands to start, stop, restart, and query the status of the service are not available. Everything else will work fine without the RootHelper.

ROOT HELPER

The root helper would normally be run first, by root. However, it doesn't really matter, as long as it is running by the time the MSPA client attempts to start, stop, restart, or query the status of the MartusServer service. It is assumed to be running on the same computer as the main MSPAServer.

The root helper does not require any data directories.

To run RootHelper, the class to execute is: `org.martus.mspa.roothelper.RootHelper`

Normally it listens on port 983. Since the whole point is to run as root, that shouldn't be a problem even on Linux boxes. However, it does support a command line option to choose a different port (`--port=1234`).

In order to have any effect, the RootHelper must be able to execute the following commands:

```
/etc/init.d/martus state
/etc/init.d/martus start
/etc/init.d/martus stop
/etc/init.d/martus restart
```

MSPASERVER

The main MSPA server class to run is: `org.martus.mspa.server.MSPAServer`

MSPAServer has data directory requirements:

```
/var/MSPAServer
/var/MSPAServer/MartusServerData/
    (Symlink to the main MartusServer data dir, typically /var/MartusServer/)
/var/MSPAServer/adminTriggers/
    (Can be empty)
/var/MSPAServer/deleteOnStartup/
    keypair.dat
    clientsWhoCallUs/
        (Contains <publiccode>.mpi files for each authorized MSPA client)
        (NOTE: .mpi must be in server format, not client format)
```

When run, it will request a password, which will be used to create the SSL cert, and will be forwarded to the RootHelper each time a start, or restart is requested.

When run as non-root on Linux systems, you must use the `--port=` command line option to avoid using the default port of 984 to listen to MSPA clients. Also, if you specified a RootHelper port, you must match it with a `--roothelper-port=` command line setting.

CLIENT SIDE

You will need to provide the MSPA server public key file to the MSPA Client users. To create the MSPA server public key file, go to the directory where you have access to the Bouncy Castle crypto file (`bc-jce.jar`), and run the following command (all one line):

```
java -Xbootclasspath/p:/usr/local/martus/jars/bc-jce.jar
org.martus.server.tools.ExportPublicKey --keypair=keypair.dat
--file=MSPApublickey
```

You will be prompted for the server passphrase, and told when the MSPA public key has been exported.

You will also need to install any public keys exported by the MSPA Client in the MSPAServer's `/chroot/etc/MSPAServer/clientsWhoCallUs` directory. When copying the client public code file to that directory, it has to be owned by 'root' and have a group association of 'mspa'. Furthermore both must have read permission on the file.

The Martus service must be stopped prior to installing the key. The public key provided by the client (probably called `publickey.txt`) should be renamed to have a filename in the following format:

`"username=publiccode-ip=ipaddress"`. For example,
`joe-code=6587.7647.2163.3431.6265-ip=10.10.220.237`