

freeIPA 1.2.1

User Guide

IPA Solutions from the IPA Experts

freeIPA

freeIPA 1.2.1 User Guide

IPA Solutions from the IPA Experts

Edition 1.0

Copyright © 2008 Red Hat. This material may only be distributed subject to the terms and conditions set forth in the Open Publication License, V1.0 or later. The latest version of the OPL is presently available at <http://www.opencontent.org/openpub/>.

Red Hat and the Red Hat "Shadow Man" logo are registered trademarks of Red Hat, Inc. in the United States and other countries.

All other trademarks referenced herein are the property of their respective owners.

The GPG fingerprint of the security@redhat.com key is:

CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

1801 Varsity Drive
Raleigh, NC 27606-2072
USA
Phone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588
Research Triangle Park, NC 27709
USA

This guide covers topics such as connecting to the IPA server, basic account management (self service), and using the IPA browser and command line interfaces.

Preface	v
1. Audience	v
2. Document Conventions	v
2.1. Typographic Conventions	v
2.2. Pull-quote Conventions	vi
2.3. Notes and Warnings	vii
3. We Need Feedback!	viii
1. Introduction to IPA	1
2. Using IPA	3
2.1. Logging in to IPA	3
2.1.1. Logging in as a Different User	3
2.2. Managing Your Account	3
2.2.1. Account Management Restrictions	3
2.2.2. Using the Web Interface (Self Service)	4
2.2.3. Using the Command-Line	4
2.3. Searching for Users and Groups	4
2.3.1. Searching for Users	5
2.3.2. Searching for Groups	6
A. Revision History	9

Preface

Welcome to the IPA User Guide. This guide provides the information necessary for the day to day usage of IPA on any of the supported client platforms.

1. Audience

The IPA User Guide is intended for end users and those involved in managing their own account information using either the web interface or the command line interface to IPA.

2. Document Conventions

This manual uses several conventions to highlight certain words and phrases and draw attention to specific pieces of information.

In PDF and paper editions, this manual uses typefaces drawn from the [Liberation Fonts](https://fedorahosted.org/liberation-fonts/)¹ set. The Liberation Fonts set is also used in HTML editions if the set is installed on your system. If not, alternative but equivalent typefaces are displayed. Note: Red Hat Enterprise Linux 5 and later includes the Liberation Fonts set by default.

2.1. Typographic Conventions

Four typographic conventions are used to call attention to specific words and phrases. These conventions, and the circumstances they apply to, are as follows.

Mono-spaced Bold

Used to highlight system input, including shell commands, file names and paths. Also used to highlight key caps and key-combinations. For example:

To see the contents of the file **my_novel1** in your current working directory, enter the **cat my_novel1** command at the shell prompt and then press **Enter**.

The above example includes a file name, a shell command and a key cap, all presented in Mono-spaced Bold and all distinguishable thanks to context.

Key-combinations can be distinguished from key caps by the hyphen connecting each part of a key-combination. For example:

Press **Enter** to execute the command.

Press **Ctrl-Alt-F1** to switch to the first virtual terminal. Press **Ctrl-Alt-F7** to return to your X-Windows session.

The first sentence highlights the particular key cap to press. The second highlights two sets of three key caps, each set pressed simultaneously.

If source code is discussed, class names, methods, functions, variable names and returned values mentioned within a paragraph will be presented as above, in **Mono-spaced Bold**. For example:

File-related classes include **filesystem** for file systems, **file** for files, and **dir** for directories. Each class has its own associated set of permissions.

¹ <https://fedorahosted.org/liberation-fonts/>

Proportional Bold

This denotes words or phrases encountered on a system, including application names; dialogue box text; labelled buttons; check-box and radio button labels; menu titles and sub-menu titles. For example:

Choose **System > Preferences > Mouse** from the main menu bar to launch **Mouse Preferences**. In the **Buttons** tab, click the **Left-handed mouse** check box and click **Close** to switch the primary mouse button from the left to the right (making the mouse suitable for use in the left hand).

The above text includes application names; system-wide menu names and items; application-specific menu names; and buttons and text found within a GUI interface, all presented in Proportional Bold and all distinguishable by context.

Note the **>** shorthand used to indicate traversal through a menu and its sub-menus. This avoids the difficult-to-follow 'Select **Mouse** from the **Preferences** sub-menu in the **System** menu of the main menu bar' approach.

Mono-spaced Bold Italic or *Proportional Bold Italic*

Whether Mono-spaced Bold or Proportional Bold, the addition of Italics indicates replaceable or variable text. Italics denotes text you do not input literally or displayed text that changes depending on circumstance. For example:

To connect to a remote machine using ssh, type **ssh *username@domain.name*** at a shell prompt. If the remote machine is **example.com** and your username on that machine is john, type **ssh *john@example.com***.

To see the version of a currently installed package, use the **rpm -q *package*** command. It will return a result as follows: ***package-version-release***.

Note the words in bold italics above — username, domain.name, package, version and release. Each word is a placeholder, either for text you enter when issuing a command or for text displayed by the system.

Aside from standard usage for presenting the title of a work, italics denotes the first use of a new or important term. For example:

When the Apache HTTP Server accepts requests, it dispatches child processes or threads to handle them. This group of child processes or threads is known as a *server-pool*. Under Apache HTTP Server 2.0, the responsibility for creating and maintaining these server-pools has been abstracted to a group of modules called *Multi-Processing Modules (MPMs)*. Unlike other modules, only one module from the MPM group can be loaded by the Apache HTTP Server.

2.2. Pull-quote Conventions

Two, commonly multi-line, data types are set off visually from the surrounding text.

Output sent to a terminal is set in Mono-spaced Roman and presented thus:

books	Desktop	documentation	drafts	mss	photos	stuff	svn
books_tests	Desktop1	downloads	images	notes	scripts	svgs	

Source-code listings are also set in Mono - spaced Roman but are presented and highlighted as follows:

```
package org.jboss.book.jca.ex1;

import javax.naming.InitialContext;

public class ExClient
{
    public static void main(String args[])
        throws Exception
    {
        InitialContext iniCtx = new InitialContext();
        Object          ref    = iniCtx.lookup("EchoBean");
        EchoHome        home   = (EchoHome) ref;
        Echo             echo   = home.create();

        System.out.println("Created Echo");

        System.out.println("Echo.echo('Hello') = " + echo.echo("Hello"));
    }
}
```

2.3. Notes and Warnings

Finally, we use three visual styles to draw attention to information that might otherwise be overlooked.



Note

A Note is a tip or shortcut or alternative approach to the task at hand. Ignoring a note should have no negative consequences, but you might miss out on a trick that makes your life easier.



Important

Important boxes detail things that are easily missed: configuration changes that only apply to the current session, or services that need restarting before an update will apply. Ignoring Important boxes won't cause data loss but may cause irritation and frustration.



Warning

A Warning should not be ignored. Ignoring warnings will most likely cause data loss.

3. We Need Feedback!

If you find a typographical error in this manual, or if you have thought of a way to make this manual better, we would love to hear from you! Please submit a report in Bugzilla: https://bugzilla.redhat.com/enter_bug.cgi?product=freeIPA against the Documentation component.

When submitting a bug report, be sure to mention the manual's identifier: *User_Guide*

If you have a suggestion for improving the documentation, try to be as specific as possible when describing it. If you have found an error, please include the section number and some of the surrounding text so we can find it easily.

Introduction to IPA

IPA provides both command-line and browser-based interfaces to the IPA server and the functionality that it provides. You can use either of these interfaces to manage various aspects of your own account, and to search for other IPA users and groups. You can also perform more extensive operations, such as modifying other user's account details, based on the permissions that your IPA Administrator has delegated.

Before you can log in to IPA, your IPA Administrator must create your Kerberos account and provide an initial password. You can then use these Kerberos credentials to log in from any machine that has been correctly configured.

Using IPA

2.1. Logging in to IPA

IPA uses the Kerberos credentials that you provide when you log in to your machine. To connect to the IPA web interface, enter the server's address in your browser. For example, `http://ipaserver.example.com`

2.1.1. Logging in as a Different User

If you log in to a machine using an account different from your IPA account, use the **kinit** command to establish your Kerberos credentials. Similarly, if you need to log in to IPA as a different user, perhaps in another user role or as the administrator, you need to replace your existing credentials with those of the new user. Typically you can only store Kerberos credentials for a single user, and they are the credentials that will be used when you log in to IPA.

For example, if your local account name is `localUser` but your IPA account name is `ipaUser`, run the following command, and enter your password when prompted:

```
$ kinit ipaUser
Password for ipaUser@EXAMPLE.COM:
```

This establishes your Kerberos credentials on the local machine. You can use the **klist** command to verify that you received a *ticket granting ticket (TGT)* from the server. This should return output similar to the following:

```
$ klist
Ticket cache: FILE:/tmp/krb5cc_500
Default principal: ipaUser@EXAMPLE.COM

Valid starting    Expires          Service principal
11/10/08 15:35:45  11/11/08 15:35:45  krbtgt/EXAMPLE.COM@EXAMPLE.COM

Kerberos 4 ticket cache: /tmp/tkt500
klist: You have no tickets cached
```

You should now be able to connect to the IPA web interface. If you were already connected to the web interface as another user, refresh the browser to display the updated details for the new user.

2.2. Managing Your Account

You can use the IPA Self Service facility via the web interface to update your own account information, including your name, display name, password, and contact details. You can also add and remove yourself from groups, according to the permissions set by the site administrator. Command-line tools are also available to perform all of the same operations.

2.2.1. Account Management Restrictions

You cannot edit all of the fields in your account, and restrictions may apply to other fields. For example, unless you are a member of the `admin` or `editors` groups, you cannot change your User

Login, E-mail Address, Account Status, or Manager. Password changes are subject to the restrictions specified in the Policy Requirements, which are maintained by your IPA Administrator. This helps to maintain the security of the system by ensuring that you only use strong passwords and that they are changed regularly.

For advice on how to create strong passwords, refer to [Creating Strong Passwords](#)¹ in the *Red Hat Enterprise Linux Deployment Guide*.

2.2.2. Using the Web Interface (Self Service)

To update your personal information, log in to IPA as described in [Section 2.1, “Logging in to IPA”](#). This provides access to the various tools needed to edit your own information.

Procedure 2.1. To update your personal information:

1. Click the **Self Service** link in the **Tasks** list on the right side of the page to display the **Edit User** page.
2. Update your personal information as required. To change your password, select the **edit protected fields** box at the top of the page to enable the **Password** fields.
3. Click **Update User** to save your changes.

A status message at the top of the page indicates the success or failure of the update.



Note

You need to manually edit each of the fields in the **Identity Details** and other sections. That is, if you change your first name or last name, perhaps due to some initial input error, you also need to update the **Full Name**, **Display Name**, and **Initials** fields as well. These fields do not automatically update.

2.2.3. Using the Command-Line

The IPA command-line tools provide all of the same functionality as the web interface. You can use the **ipa-moduser** command to modify any of your personal details. The syntax of this command is as follows:

```
ipa-moduser [ options ] { user }
```

You can run the command with no arguments to enter interactive mode.

The options, restrictions, and requirements described for the web interface also apply to the command-line tools. Refer to the **ipa-moduser** man page for more information.

2.3. Searching for Users and Groups

IPA provides extensive search capabilities, which enable you to perform simple and partial-match searches on a range of attributes, including:

¹ http://www.redhat.com/docs/manuals/enterprise/RHEL-5-manual/en-US/RHEL510/Deployment_Guide/s2-wstation-pass-create.html

- First Name (givenname)
- Last Name (sn)
- Login (uid)
- Job Title (title)
- Organizational Unit Name (ou)
- Phone Number (telephoneNumber)

Searches are case-insensitive, and automatically search across multiple fields. Search results are displayed with exact matches listed first, followed by partial matches.

The default display lists users in alphabetical order. Click any column title to sort in alphabetical or numerical order. Click the title again to sort in reverse order. The sort order is indicated by an icon next to the title.

Not all fields are indexed for searching. For example, you cannot search on the following user details:

- Initials
- Account Status
- Home Directory
- Login Shell
- Gecos
- Home Page



Note

You cannot use wildcards to search for users or groups. The search string must include at least one character that appears in one of the indexed search fields.

2.3.1. Searching for Users

2.3.1.1. Using the Web Interface

Procedure 2.2. To search for users using the web interface:

1. Navigate to the IPA homepage, and click **Find User** in the **Tasks** list on the right side of the page to display the **Find User** page.
2. In the text box, type all or part of the name of the user that you want to search for, and click **Find User**. If you are unsure of the user's name, enter some other keywords associated with the user.

For example:

- To find Joe Blake in the Research department, type "joe blake research" (without the quotes) in the text box.

- To find who has a particular telephone extension, type part or all of the extension in the text box.

2.3.1.2. Using the Command Line

Use the **ipa-finduser** command to search for users from the command line. The basic syntax of this command is as follows:

ipa-finduser [options] { string }



Note

Unlike the web version of the Find User utility, you can only search for a single string using the command-line version.

Refer to the **ipa-finduser** man page for more information on the options available.

The following example demonstrates using the **ipa-finduser** command to find users whose record contains the string "park":

```
$ /usr/sbin/ipa-finduser park
2 entries were found. Which one would you like to display?
1: Julie Park (parkj)
2: Jackson Park (jpark)
Choose one: (1 - 2), 0 for all, q to quit: 1
First Name: Julie
Last Name: Park
Home Directory: /home/parkj
Login Shell: /bin/bash
Login: parkj
```

2.3.2. Searching for Groups

2.3.2.1. Using the Web Interface

Procedure 2.3. To search for groups using the web interface:

1. Navigate to the IPA homepage, and click the **Find Group** link in the **Tasks** list on the right side of the page to display the **Find Group** page.
2. Type the keywords that you want to search for in the text box, and click **Find Group**.



Note

You cannot search on quoted strings. For example, you cannot search for an exact match on "Engineering Group Members".

2.3.2.2. Using the Command Line

Use the **ipa-findgroup** command to search for groups from the command line. The basic syntax of this command is as follows:

ipa-findgroup { string }



Note

Unlike the web version of the Find Group utility, you can only search for a single string using the command-line version.

Refer to the **ipa-findgroup** man page for more information on the options available.

The following example demonstrates using the **ipa-findgroup** command to find groups that contain the string "Documentation":

```
$ /usr/sbin/ipa-findgroup Documentation
3 entries were found. Which one would you like to display?
1: Documentation
2: Writers
3: Translators
Choose one: (1 - 3), 0 for all, q to quit: 1
dn: cn=Documentation,cn=groups,cn=accounts,dc=example,dc=com
GID: 1108
Full Name: Documentation
Description: All documentation group members and sub-groups
Members:
David Kim: uid=dkim,cn=users,cn=accounts,dc=example,dc=com
Kay Lee: uid=klee,cn=users,cn=accounts,dc=example,dc=com
Namjo Kang: uid=nkang,cn=users,cn=accounts,dc=example,dc=com
Anna Belle: uid=abelle,cn=users,cn=accounts,dc=example,dc=com
Shohei Joi: uid=sjoi,cn=users,cn=accounts,dc=example,dc=com
Writers: cn=Writers,cn=groups,cn=accounts,dc=example,dc=com
Translators: cn=Translators,cn=groups,cn=accounts,dc=example,dc=com
```



Note

The **ipa-findgroup** command searches both group names and group descriptions. If your search results are too extensive, use a more specific search string.

Appendix A. Revision History

Revision 1.1 Tue Nov 02 2008 David O'Brien davido@redhat.com

BZ 470721. Updates from tech review.

BZ 451318. Document behavior of name changes using ipa-moduser.

BZ 470711. Document how to log in as a different user.

BZ 468209.

Updates to section Using the Web Interface.

Updates to section Searching for Users and Groups.

Add section on using cli for user updates.

Revision 1.0 Tue Jul 01 2008 David O'Brien davido@redhat.com

Created

