freeIPA 1.2.1

Client Configuration Guide

IPA Solutions from the IPA Experts

freeIPA

freeIPA 1.2.1 Client Configuration Guide
IPA Solutions from the IPA Experts
Edition 1.0

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 describes how to configure IPA on each of the supported client platforms.

Preface

Welcome to the IPA Client Configuration Guide. This guide provides you with the information necessary to configure each of the supported client platforms to connect to the IPA server. This includes:

- System login (for accounts that exist in the IPA server)
- `NFS` v4 with `Kerberos` (for mounting remote file systems)
- `SSH` access (secure client system access with `Kerberos`)
- Using **Firefox** to access the IPA web interface (for administrative operations)

1. Audience

The IPA Client Configuration Guide is intended for system administrators and those responsible for ensuring the successful configuration of IPA clients.

This guide assumes a good understanding of various operating systems, including `Linux`, `Solaris` and other UNIX systems, `Macintosh` and Microsoft `Windows`. It also assumes a working knowledge of `LDAP` and either Red Hat or Fedora Directory Server.

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*[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_novel`** in your current working directory, enter the **`cat my_novel`** 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:

[1] https://fedorahosted.org/liberation-fonts/

> 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.

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: *Client_Configuration_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.

Configuring Red Hat Enterprise Linux Clients

This chapter describes how to configure Red Hat Enterprise Linux as an IPA client. Refer to the IPA *Release Notes* for the currently supported versions of Red Hat Enterprise Linux.

Before starting the IPA installation, update your system with all the latest packages.

> **Note**
>
> The IPA client installation process requires that an IPA server already exist.
>
> Many of the following procedures and instructions use example host names, domain names, and realm names for illustration purposes. You need to replace these example names with those that apply to your own deployment.

1.1. Configuring Red Hat Enterprise Linux 5 as an IPA Client

> **Important**
>
> The following instructions assume that you have purchased a subscription to the Red Hat Enterprise IPA channel. freeIPA does not provide client packages for Red Hat Enterprise Linux.

1.1.1. Downloading and Installing the IPA Packages

The most efficient way to install the required client packages is to use your IPA master as a yum repository. You can then install the client packages directly from the IPA master. Refer to the *Setting up the IPA Server* chapter in the IPA Installation and Deployment Guide for information on how to set up the IPA master.

Procedure 1.1. To install the Red Hat Enterprise Linux 5 IPA packages:

1. - For a user workstation, run the following command: `# yum install ipa-client`
   - For an administrator's workstation, run the following command: `# yum install ipa-client ipa-admintools`
2. If the IPA server is also configured as the DNS server, and is in the same domain as the client, add the server's IP address as the first entry in the client's **`/etc/resolv.conf`** file.

1.1.2. Configuring Client Authentication

Procedure 1.2. To configure client authentication on Red Hat Enterprise Linux 5, run the following command:

- `# ipa-client-install`

If DNS Discovery is configured correctly, the script should set up the client without prompting for any further information. This includes configuring the name service cache daemon (nscd) to start at boot time. The nscd caches the most common name service requests from the client, and reduces the load on the server. If DNS Discovery is not configured, the script will prompt you for the information it requires.

When the script has finished configuring the IPA client, it displays information about the realm, DNS domain, IPA server, and other related information, similar to the following:

```
Discovery was successful!
Realm: EXAMPLE.COM
DNS Domain: example.com
IPA Server: ipaserver.example.com
BaseDN: dc=example,dc=com
```

> **Note**
>
> Ensure that you run the correct command to set up the client. Separate scripts exist for Red Hat Enterprise Linux 4 and 5, and they are not interchangeable.
>
> If the IPA server and client are not in the same domain, the setup script will prompt you for the information that it requires.

1.1.3. Configuring Kerberos

The installation script performs the Kerberos configuration automatically. This includes specifying the realm and domain details, and default ticket attributes. Forwardable tickets are configured by default, which facilitates connection to the administration interface from any operating system, and also provides for auditing of administration operations.

The following is an example of a Kerberos configuration file for IPA:

```
[libdefaults]
default_realm = EXAMPLE.COM
dns_lookup_realm = true
dns_lookup_kdc = true
forwardable = yes
ticket_lifetime = 24h

[realms]
EXAMPLE.COM = {
 kdc = ipaserver.example.com:88
 admin_server = ipaserver.example.com:749
 default_domain = example.com
 }
[domain_realm]
.example.com = EXAMPLE.COM
example.com = EXAMPLE.COM
```

1.1.4. Configuring Client TLS

The SSL/TLS settings are only required if you want to use SSL between the clients and the server when performing operations such as account lookups.

Procedure 1.3. To configure a Red Hat Enterprise Linux 5 client for TLS:

1. Make the following changes to the **`/etc/ldap.conf`** file:

   ```
   uri            ldap://ipaserver.example.com/
   base           dc=example,dc=com
   ssl            start_tls
   tls_checkpeer  yes
   tls_cacertdir  /etc/cacerts/
   ```

   > **Note**
   >
   > Ensure that the directory you specify for `tls_cacertdir` actually exists.
   >
   > If the `tls_cacertdir` directive does not work, run the following command to set the cacert file directly:
   >
   > ```
   > # tls_cacert /etc/cacerts/cacert.crt
   > ```

2. Log in to the client machine, and change to the `root` user.

3. Change to the directory where you need to install the CA certificate.

   ```
   # cd /etc/cacerts
   ```

4. Run the following command to copy the CA certificate from the server to the client:

   ```
   # wget http://ipaserver.example.com/ipa/config/ca.crt
   ```

   If you installed IPA using your own PKCS#12 files then this self-signed CA will not exist.

5. Install the CA certificate as follows:

   ```
   # cp cacert.crt /etc/cacerts/`openssl x509 -noout -hash -in
   cacert.crt`.0
   ```

   The resulting file name is the hash of the contents of the certificate with a ".0" extension.

6. If more than one CA certificate is required, concatenate these certificates into a single file.

Refer to *http://directory.fedora.redhat.com/wiki/Howto:SSL* for more information on TLS Client Configuration for Linux clients.

1.1.5. Configuring System Login

No additional configuration is required to enable system login on Red Hat Enterprise Linux 5. Use the following tests to ensure that the configuration is working correctly:

- On the system console, log in as an IPA user. After you have logged in, open a shell and run the following commands:

  $ id (ensure that the user IDs and group IDs are correct)

  ```
  $ getent passwd <userid>
  ```

  ```
  $ getent group ipausers
  ```

If any of these tests fail, refer to the Troubleshooting section in the *Administration Guide* for information on how to locate any problems.

1.1.6. Configuring NFS v4 with Kerberos

Procedure 1.4. To configure NFS on the Red Hat Enterprise Linux 5 IPA client:

1. Obtain a `Kerberos` ticket for the `admin` user.

   ```
   # kinit admin
   ```

2. Add an `NFS` service principal on the client.

   ```
   # ipa-addservice nfs/ipaclient.example.com
   ```

3. Obtain a keytab for the `NFS` service principal.

   ```
   # ipa-getkeytab -s ipaserver.example.com -p nfs/ipaclient.example.com -k /etc/krb5.keytab
   ```

   > **Note**
   >
   > The Linux `NFS` implementation still has limited encryption type support. If your NFS server is hosted on a Linux machine, you may need to use the `-e des-cbc-crc` option to the **`ipa-getkeytab`** command for any nfs/<FQDN> service keytabs you want to set up, both on the server and on all clients. This instructs the KDC to generate only DES keys.

4. Add the following line to the **`/etc/sysconfig/nfs`** file:

   ```
   SECURE_NFS=yes
   ```

5. Start the `rpcgssd` daemon.

   ```
   # service rpcgssd start
   ```

The IPA client should now be fully configured to mount `NFS` shares using `Kerberos` credentials. Use the following command to test the configuration:

```
# mount -v -t nfs4 -o sec=krb5 ipaserver.example.com:/ /mnt
```

1.1.7. Configuring Client SSH Access

You can also configure the IPA client to accept incoming `SSH` requests and authenticate with the user's `Kerberos` credentials. After configuring the IPA client, use the following procedure to configure the IPA client for `SSH` connections. Remember to replace the example host and domain names with your own host and domain name.

Procedure 1.5. To configure a Red Hat Enterprise Linux 5 IPA client for incoming SSH connections:

1. The IPA client installation process configures the `NTP` service by default, but you should ensure that time on the IPA client and server is synchronized. If it is not, run the following commands on the IPA client:

   ```
   # service ntpd stop
   ```

   ```
   # ntpdate -s -p 8 -u ipaserver.example.com
   ```

   ```
   # service ntpd start
   ```

   > **Note**
   >
   > The **`ntpdate`** command does not work if `ntpd` is running.

2. Obtain a `Kerberos` ticket for the `admin` user.

   ```
   # kinit admin
   ```

3. Add a `host` service principal on the IPA client.

   ```
   # ipa-addservice host/ipaclient.example.com
   ```

4. Retrieve the keytab.

   ```
   # ipa-getkeytab -s ipaserver.example.com -p host/ipaclient.example.com -
   k /etc/krb5.keytab
   ```

The IPA client should now be fully configured to accept incoming `SSH` connections and authenticate with the user's `Kerberos` credentials. Use the following command on another machine to test the configuration. This should succeed without asking for a password.

```
# ssh admin@ipaclient.example.com
```

1.1.8. Configuring Host-Based Access Control

You can configure Red Hat Enterprise Linux and Fedora to allow or deny access to IPA resources and services based on the configuration of the host from which access is attempted. Refer to the Configuring Access Control chapter of the *Administration Guide* for information on this topic.

1.2. Configuring Red Hat Enterprise Linux 4 as an IPA Client

Important

The following instructions assume that you have purchased a subscription to the Red Hat Enterprise IPA channel. freeIPA does not provide client packages for Red Hat Enterprise Linux.

1.2.1. Downloading and Installing the IPA Packages

Download and install the Red Hat Enterprise Linux 4 IPA Client RPM from the "Downloads" section of the appropriate Red Hat Enterprise IPA channel on the Red Hat Network.

1.2.2. Configuring Client Authentication

Procedure 1.6. To configure client authentication on Red Hat Enterprise Linux 4:

1. Create the **`/etc/ipa/ipa.conf`** file.

2. Use the following command to set up the IPA client:

   ```
   # ipa-client-setup --server ipaserver.example.com
   ```

3. Reboot the client machine.

Note

Ensure that you run the correct command to set up the client. Separate scripts exist for Red Hat Enterprise Linux 4 and 5, and they are not interchangeable.

The Red Hat Enterprise Linux 4 version of the IPA client installation script does not perform auto-discovery, and neither does it configure the client machine to perform auto-discovery.

1.2.3. Configuring Kerberos

The installation script performs the `Kerberos` configuration automatically. This includes specifying the realm and domain details, and default ticket attributes. Forwardable tickets are configured by default, which facilitates connection to the administration interface from any operating system, and also provides for auditing of administration operations.

The following is an example of a `Kerberos` configuration file for IPA:

```
[libdefaults]
default_realm = EXAMPLE.COM
dns_lookup_realm = true
dns_lookup_kdc = true
```

```
forwardable = yes
ticket_lifetime = 24h

[realms]
EXAMPLE.COM = {
 kdc = ipaserver.example.com:88
 admin_server = ipaserver.example.com:749
 default_domain = example.com
 }
[domain_realm]
.example.com = EXAMPLE.COM
example.com = EXAMPLE.COM
```

1.2.4. Configuring Client TLS

The SSL/TLS settings are only required if you want to use SSL between the clients and the server when performing operations such as account lookups.

Procedure 1.7. To configure a Red Hat Enterprise Linux 4 client for TLS:

1. Make the following changes to the **/etc/ldap.conf** file:

   ```
   uri             ldap://ipaserver.example.com/
   base            dc=example,dc=com
   ssl             start_tls
   tls_checkpeer   yes
   tls_cacertdir   /etc/cacerts/
   ```

   > **Note**
   >
   > Ensure that the directory you specify for `tls_cacertdir` actually exists.
   >
   > If the `tls_cacertdir` directive does not work, run the following command to set the cacert file directly:
   >
   > ```
   > # tls_cacert /etc/cacerts/cacert.crt
   > ```

2. Log in to the client machine, and change to the `root` user.

3. Change to the directory where you need to install the CA certificate.

   ```
   # cd /etc/cacerts
   ```

4. Run the following command to copy the CA certificate from the server to the client:

   ```
   # wget http://ipaserver.example.com/ipa/config/ca.crt
   ```

   If you installed IPA using your own PKCS#12 files then this self-signed CA will not exist.

5. Install the CA certificate as follows:

   ```
   # cp cacert.crt /etc/cacerts/`openssl x509 -noout -hash -in
   cacert.crt`.0
   ```

   The resulting file name is the hash of the contents of the certificate with a ".0" extension.

6. If more than one CA certificate is required, concatenate these certificates into a single file.

Refer to *http://directory.fedora.redhat.com/wiki/Howto:SSL* for more information on TLS Client Configuration for Linux clients.

1.2.5. Configuring System Login

No additional configuration is required to enable system login on Red Hat Enterprise Linux 4. Use the following tests to ensure that the configuration is working correctly:

- On the system console, log in as an IPA user. After you have logged in, open a shell and run the following commands:

  `$ id` (ensure that the user IDs and group IDs are correct)

  ```
  $ getent passwd <userid>
  ```

  ```
  $ getent group ipausers
  ```

If any of these tests fail, refer to the Troubleshooting section in the *Administration Guide* for information on how to locate any problems.

1.2.6. Configuring NFS v4 with Kerberos

Procedure 1.8. To configure NFS on the Red Hat Enterprise Linux 4 IPA client:

1. Obtain a `Kerberos` ticket for the `admin` user.

   ```
   # kinit admin
   ```

2. The *ipa-admintools* package is not available for Red Hat Enterprise Linux 4. Consequently, you need to perform the following steps on the IPA server.

   a. Add an NFS service principal for the client.

   ```
   # ipa-addservice nfs/ipaclient.example.com
   ```

   b. Retrieve the NFS keytab.

   ```
   # ipa-getkeytab -s ipaserver.example.com -p nfs/
   ipaclient.example.com -k /tmp/krb5.keytab
   ```

   `# klist -ket /tmp/krb5.keytab` (to verify)

   > **Note**
   >
   > The Linux NFS implementation still has limited encryption type support. If your NFS server is hosted on a Linux machine, you may need to use the `-e des-cbc-crc` option to the **`ipa-getkeytab`** command for any nfs/<FQDN> service keytabs you want to set up, both on the server and on all clients. This instructs the KDC to generate only DES keys.

   c. Copy the keytab from the server to the client.

   ```
   # scp /tmp/krb5.keytab root@ipaclient.example.com:/tmp/krb5.keytab
   ```

3. On the IPA client, use the **`ktutil`** command to import the keytab.

   ```
   # ktutil
   ktutil: read_kt /tmp/krb5.keytab
   ktutil: write_kt /etc/krb5/krb5.keytab
   ktutil: q
   ```

4. Add the following line to the **`/etc/sysconfig/nfs`** file:

   ```
   SECURE_NFS=yes
   ```

5. Start the `rpcgssd` daemon.

   ```
   # service rpcgssd start
   ```

The IPA client should now be fully configured to mount NFS shares using `Kerberos` credentials. Use the following command to test the configuration:

```
# mount -v -t nfs4 -o sec=krb5 ipaserver.example.com:/ /mnt
```

1.2.7. Configuring Client SSH Access

You can configure the IPA client to accept incoming SSH requests and authenticate with the user's `Kerberos` credentials. After installing and configuring the IPA client, use the following procedure to configure the IPA client for SSH connections. Remember to replace the example host and domain names with your own host and domain name.

Procedure 1.9. To configure a Red Hat Enterprise Linux 4 IPA client for incoming SSH connections:

1. The IPA client installation process configures the `NTP` service by default, but you should ensure that time on the IPA client and server is synchronized. If it is not, run the following commands on the IPA client:

   ```
   # service ntpd stop
   ```

   ```
   # ntpdate -s -p 8 -u ipaserver.example.com
   ```

   ```
   # service ntpd start
   ```

   > **Note**
   >
   > The **`ntpdate`** command does not work if `ntpd` is running.

2. Obtain a `Kerberos` ticket for the `admin` user.

   ```
   # kinit admin
   ```

3. The *ipa-admintools* package is not available for Red Hat Enterprise Linux 4. Consequently, you need to perform the following commands on the IPA server.

   a. Add a `host` service principal.

      ```
      # ipa-addservice host/ipaclient.example.com
      ```

   b. Retrieve the host keytab.

      ```
      # ipa-getkeytab -s ipaserver.example.com -p host/
      ipaclient.example.com -k /tmp/krb5.keytab
      ```

   c. Copy the keytab from the server to the client.

      ```
      # scp /tmp/krb5.keytab root@ipaclient.example.com:/tmp/krb5.keytab
      ```

4. On the IPA client, use the **`ktutil`** command to import the keytab.

   ```
   # ktutil
   ktutil: read_kt /tmp/krb5.keytab
   ktutil: write_kt /etc/krb5/krb5.keytab
   ktutil: q
   ```

The IPA client should now be fully configured to accept incoming `SSH` connections and authenticate with the user's `Kerberos` credentials. Use the following command on another machine to test the configuration. This should succeed without asking for a password.

```
# ssh admin@ipaclient.example.com
```

1.2.8. Configuring Host-Based Access Control

You can configure Red Hat Enterprise Linux and Fedora to allow or deny access to IPA resources and services based on the configuration of the host from which access is attempted. Refer to the Configuring Access Control chapter of the *Administration Guide* for information on this topic.

1.3. Configuring Red Hat Enterprise Linux 2.1 and 3 as IPA Clients

The following procedures describe how to configure Red Hat Enterprise Linux 2.1 and 3 as IPA clients. The procedures are the same for each. There are no IPA packages or installation scripts for either of these distributions; the process is completely manual.

> **Note**
>
> The IPA client installation process requires that an IPA server already exist.

1.3.1. Configuring Kerberos

Procedure 1.10. To set up client authentication:

1. Run **`authconfig`** as the root user.

2. On the **User Information Configuration** screen, select **LDAP**, and enter the server name and *`Base DN`*.

   > **Note**
   >
   > The *`Base DN`* is the realm name translated into "dc" components. For example:
   >
   > EXAMPLE.COM -> dc=example,dc=com
   >
   > This step does not fully configure *nss_ldap*. Further configuration is described below.

3. Navigate to the **Authentication Configuration** screen.

4. Ensure that **Use LDAP Authentication** is *not* selected.

5. Select **Use Kerberos 5** and enter the following details (modify to suit your deployment):

   ```
   Realm: EXAMPLE.COM
   KDC: ipaserver.example.com:88
   Admin Server: ipaserver.example.com:749
   ```

6. Press **`Enter`** to save the configuration and exit the **`authconfig`** utility.

1.3.2. Configuring LDAP

Make the following configuration changes to the **/etc/ldap.conf** file to complete the client configuration for Red Hat Enterprise Linux 3. Modify the examples provided to suit your deployment. You may need to add some of these entries if they do not exist in the original file.

```
ldap_version 3
host ipaserver.example.com
base dc=example,dc=com

nss_base_passwd cn=users,cn=accounts,dc=example,dc=com?sub
nss_base_group cn=groups,cn=accounts,dc=example,dc=com?sub
nss_schema rfc2307bis
nss_map_attribute uniqueMember member
nss_initgroups_ignoreusers root

nss_reconnect_maxsleeptime 8
nss_reconnect_sleeptime 1
bind_timelimit 5
timelimit 15

ssl no
```

This completes the configuration steps for IPA.

Note

The latest version of Red Hat Enterprise Linux 3 uses *openssh 3.6.1p2* by default, which does not support the use of `Kerberos` 5 authentication unless a special patch provided by GSS is installed. This affects both the SSH client and the SSH daemon.

Consequently, IPA users on Red Hat Enterprise Linux 3 cannot perform passwordless login to an IPA server, and other IPA servers and clients cannot perform passwordless login to a Red Hat Enterprise Linux 3 machine.

Chapter 2.

Configuring Fedora as an IPA Client

This chapter describes how to configure Fedora as an IPA client. Refer to the IPA *Release Notes* for the currently supported versions of Fedora.

Before starting the IPA installation, ensure that you update your system with all the latest packages.

> **Note**
>
> The IPA client installation process requires that an IPA server already exist.
>
> Many of the following procedures and instructions use example host names, domain names, and realm names for illustration purposes. You need to replace these example names with those that apply to your own deployment.

2.1. Downloading and Installing the IPA Packages

Procedure 2.1. To download and install the Fedora IPA packages and dependencies:

1. Install the appropriate IPA client packages:

   - For a user workstation, run the following command:

     ```
     # yum install ipa-client
     ```

   - For an administrator's workstation, run the following command:

     ```
     # yum install ipa-client ipa-admintools
     ```

2. If the IPA server is also configured as the DNS server, and is in the same domain as the client, add the server's IP address as the first entry in the client's **`/etc/resolv.conf`** file.

2.2. Configuring Client Authentication

Procedure 2.2. To configure client authentication on Fedora:

- Run the following command to set up the IPA client:

  ```
  # ipa-client-install
  ```

If `DNS` Discovery is configured correctly, the script should set up the client without prompting for any further information. This includes configuring the name service cache daemon (nscd) to start at boot time. The `nscd` caches the most common name service requests from the client, and reduces the load on the server. If `DNS` Discovery is not configured, the script will prompt you for the information it requires.

When the script has finished configuring the IPA client, it displays information about the realm, DNS domain, IPA server, and other related information, similar to the following:

```
Discovery was successful!
```

```
Realm: EXAMPLE.COM
DNS Domain: example.com
IPA Server: ipaserver.example.com
BaseDN: dc=example,dc=com
```

Note

If the IPA server and client are not in the same domain, the setup script will prompt you for the information that it requires.

2.3. Configuring Kerberos

The installation script performs the Kerberos configuration automatically. This includes specifying the realm and domain details, and default ticket attributes. Forwardable tickets are configured by default, which facilitates connection to the administration interface from any operating system, and also provides for auditing of administration operations.

The following is an example of a Kerberos configuration file for IPA:

```
[libdefaults]
default_realm = EXAMPLE.COM
dns_lookup_realm = true
dns_lookup_kdc = true
forwardable = yes
ticket_lifetime = 24h

[realms]
EXAMPLE.COM = {
 kdc = ipaserver.example.com:88
 admin_server = ipaserver.example.com:749
 default_domain = example.com
 }
[domain_realm]
.example.com = EXAMPLE.COM
example.com = EXAMPLE.COM
```

2.4. Configuring Client TLS

The SSL/TLS settings are only required if you want to use SSL between the clients and the server when performing operations such as account lookups.

Procedure 2.3. To configure a Fedora client for TLS:

1. Make the following changes to the **/etc/ldap.conf** file:

   ```
   uri             ldap://ipaserver.example.com/
   base            dc=example,dc=com
   ssl             start_tls
   tls_checkpeer   yes
   tls_cacertdir   /etc/cacerts/
   ```

   Note

   Ensure that the directory you specify for `tls_cacertdir` actually exists.

   If the `tls_cacertdir` directive does not work, run the following command to set the cacert file directly:

   ```
   # tls_cacert /etc/cacerts/cacert.crt
   ```

2. Log in to the client machine, and change to the `root` user.

3. Change to the directory where you need to install the CA certificate.

   ```
   # cd /etc/cacerts
   ```

4. Run the following command to copy the CA certificate from the server to the client:

   ```
   # wget http://ipaserver.example.com/ipa/config/ca.crt
   ```

   If you installed IPA using your own PKCS#12 files then this self-signed CA will not exist.

5. Install the CA certificate as follows:

   ```
   # cp cacert.crt /etc/cacerts/`openssl x509 -noout -hash -in
   cacert.crt`.0
   ```

   The resulting file name is the hash of the contents of the certificate with a ".0" extension.

6. If more than one CA certificate is required, concatenate these certificates into a single file.

Refer to *http://directory.fedora.redhat.com/wiki/Howto:SSL* for more information on TLS Client Configuration for Linux clients.

2.5. Configuring System Login

No additional configuration is required to enable system login on Fedora. Use the following tests to ensure that the configuration is working correctly:

- On the system console, log in as an IPA user. After you have logged in, open a shell and run the following commands:

  $ id (ensure that the user IDs and group IDs are correct)

```
$ getent passwd <userid>
```

```
$ getent group ipausers
```

If any of these tests fail, refer to the Troubleshooting section in the *Administration Guide* for information on how to locate any problems.

2.6. Configuring NFS v4 with Kerberos

Procedure 2.4. To configure NFS on the Fedora IPA client:

1. Obtain a `Kerberos` ticket for the `admin` user.

   ```
   # kinit admin
   ```

2. Add an NFS service principal on the client.

   ```
   # ipa-addservice nfs/ipaclient.example.com
   ```

3. Obtain a keytab for the NFS service principal.

   ```
   # ipa-getkeytab -s ipaserver.example.com -p nfs/ipaclient.example.com -
   k /etc/krb5.keytab
   ```

   > **Note**
   >
   > The Linux NFS implementation still has limited encryption type support. If your NFS server is hosted on a Linux machine, you may need to use the `-e des-cbc-crc` option to the **`ipa-getkeytab`** command for any nfs/<FQDN> service keytabs you want to set up, both on the server and on all clients. This instructs the KDC to generate only DES keys.

4. Add the following line to the **`/etc/sysconfig/nfs`** file:

   ```
   SECURE_NFS=yes
   ```

5. Start the `rpcgssd` daemon.

   ```
   # service rpcgssd start
   ```

The IPA client should now be fully configured to mount NFS shares using `Kerberos` credentials. Use the following command to test the configuration:

```
# mount -v -t nfs4 -o sec=krb5 ipaserver.example.com:/ /mnt
```

2.7. Configuring Client SSH Access

You can also configure the IPA client to accept incoming SSH requests and authenticate with the user's `Kerberos` credentials. After installing and configuring the IPA client, use the following procedure to configure the IPA client for SSH connections. Remember to replace the example host and domain names with your own host and domain name.

Procedure 2.5. To configure a Fedora IPA client for incoming SSH connections:

1. The IPA client installation process configures the `NTP` service by default, but you should ensure that time on the IPA client and server is synchronized. If it is not, run the following commands on the IPA client:

   ```
   # service ntpd stop
   ```

   ```
   # ntpdate -s -p 8 -u ipaserver.example.com
   ```

   ```
   # service ntpd start
   ```

   > **Note**
   >
   > The **`ntpdate`** command does not work if `ntpd` is running.

2. Obtain a `Kerberos` ticket for the `admin` user.

   ```
   # kinit admin
   ```

3. Add a `host` service principal on the IPA client.

   ```
   # ipa-addservice host/ipaclient.example.com
   ```

4. Retrieve the keytab.

   ```
   # ipa-getkeytab -s ipaserver.example.com -p host/ipaclient.example.com -
   k /etc/krb5.keytab
   ```

The IPA client should now be fully configured to accept incoming `SSH` connections and authenticate with the user's `Kerberos` credentials. Use the following command on another machine to test the configuration. This should succeed without asking for a password.

```
# ssh admin@ipaclient.example.com
```

2.8. Configuring Host-Based Access Control

You can configure Red Hat Enterprise Linux and Fedora to allow or deny access to IPA resources and services based on the configuration of the host from which access is attempted. Refer to the Configuring Access Control chapter of the *Administration Guide* for information on this topic.

Configuring Solaris as an IPA Client

This chapter describes how to configure the various supported Solaris operating systems as IPA clients. IPA is supported on the following Solaris platforms:

- Solaris 8, 9 & 10 (SPARC)
- Solaris 10 (x86)

> **Note**
>
> Earlier versions of IPA required the use of specific *nss_ldap* packages that were made available on the freeipa.org wiki. As of freeIPA 1.2.1, this is no longer the case. Instead, you can use the native Solaris *nss_ldap* package and configure it to use the appropriate IPA services.
>
> If you are already using the above *nss_ldap* packages, you can run the following command as root to restore the system to its previous state. You can then proceed to use the native Solaris packages.
>
> ```
> # pkgrm RHATnss-ldap
> ```

3.1. Configuring Solaris 10 as an IPA Client

The following procedures describe how to configure Solaris 10 as a client for IPA. This requires modifications to the PAM, LDAP, and Kerberos configuration files. This section also includes instructions for configuring NFS, however this configuration is optional.

3.1.1. Prerequisite Configuration

Before you proceed with the main configuration, ensure that you make the following updates to your Solaris system:

Configuring NTP

Ensure that NTP is correctly configured and enabled, and that time is synchronized between the client and the IPA server.

Configuring DNS

Configure the **/etc/resolv.conf** file to include the correct DNS server. This server must be able to resolve the IPA Solaris client and IPA server names.

The following is an example of a valid **/etc/resolv.conf** file:

```
search example.com
nameserver bindserver.example.com
```

Configuring Name Service Switch (NSS)

Configure the **/etc/nsswitch.conf** file to perform password and group lookup using LDAP.

The **/etc/nsswitch.conf** file should include the following lines:

```
passwd: files ldap[NOTFOUND=return]
group: files ldap[NOTFOUND=return]
```

3.1.2. Configuring PAM

Configure the **/etc/pam.conf** file to use PAM Kerberos first.

The following example shows how to set up PAM Kerberos authentication for console login:

```
login auth requisite pam_authtok_get.so.1
login auth sufficient pam_krb5.so.1
login auth required pam_dhkeys.so.1
login auth required pam_unix_cred.so.1
login auth required pam_unix_auth.so.1 use_first_pass
login auth required pam_dial_auth.so.1
```

3.1.3. Configuring LDAP

Configure the **/etc/ldap.conf** file as follows:

```
ldap_version 3
base cn=compat,dc=example,dc=com
nss_base_passwd cn=users,cn=compat,dc=example,dc=com?sub
nss_base_group cn=groups,cn=compat,dc=example,dc=com?sub
nss_schema rfc2307bis
nss_map_objectclass shadowAccount posixAccount
nss_map_attribute uniqueMember member
nss_initgroups_ignoreusers root,dirsrv
nss_reconnect_maxsleeptime 8
nss_reconnect_sleeptime 1
bind_timelimit 5
timelimit 15
nss_srv_domain example.com
uri ldap://ipaserver.example.com
```

3.1.4. Configuring Kerberos

Configure the **/etc/krb5/krb5.conf** file as follows:

```
[libdefaults]
default_realm = EXAMPLE.COM

[realms]
EXAMPLE.COM = {
 kdc = ipaserver.example.com:88
 admin_server = ipaserver.example.com:749
 }
```

```
[domain_realm]
.example.com = EXAMPLE.COM
example.com = EXAMPLE.COM

[logging]
default = FILE:/var/krb5/kdc.log
kdc = FILE:/var/krb5/kdc.log
kdc_rotate = {
 period = 1d
 versions = 10
 }

[appdefaults]
kinit = {
 renewable = true
 forwardable= true
 }
```

The `Kerberos` configuration includes specifying the realm and domain details, and default ticket attributes. Forwardable tickets are configured by default, which facilitates connection to the administration interface from any operating system, and also provides for auditing of administration operations.

3.1.5. Configuring Client SSH Access

Use the following procedure to configure the `Solaris` IPA client to accept incoming SSH requests and authenticate with the user's `Kerberos` credentials. Remember to replace the example host and domain names with your own host and domain name.

The *ipa-admintools* package is not available for Solaris. Consequently, you need to perform the following steps on the IPA server.

Procedure 3.1. To configure client SSH access:

1. Add a `host` service principal for the `Solaris` client.

   ```
   # ipa-addservice host/solarisipaclient.example.com
   ```

2. Create the `host` keytab file.

   ```
   # ipa-getkeytab -s ipaserver.example.com -p host/
   solarisipaclient.example.com -k /tmp/krb5.keytab -e des-cbc-crc
   ```

3. Copy this keytab to the `Solaris` machine as **`/etc/krb5/krb5.keytab`**.

   ```
   # scp /tmp/krb5.keytab root@solarisipaclient.example.com:/etc/krb5/
   krb5.keytab
   ```

Note

After you have performed all of the preceding configuration steps, reboot the `Solaris` machine to ensure that all of the changes take effect.

3.1.6. Configuring NFS v4

> **Note**
>
> The NFS v4 configuration is only supported on Solaris 10.

Procedure 3.2. To configure NFS on the Solaris IPA client:

1. Obtain a `Kerberos` ticket for the `admin` user.

   ```
   # kinit admin
   ```

2. The *ipa-admintools* package is not available for Solaris. Consequently, you need to perform the following steps on the IPA server.

   a. Add an `NFS` service principal for the client.

      ```
      # ipa-addservice nfs/solarisipaclient.example.com
      ```

   b. Create the `NFS` keytab file.

      ```
      # ipa-getkeytab -s ipaserver.example.com -p nfs/solarisipaclient.example.com -k /tmp/krb5.keytab -e des-cbc-crc
      ```

      `# klist -ket /tmp/krb5.keytab` (to verify)

      > **Note**
      >
      > The Linux `NFS` implementation still has limited encryption type support. If your NFS server is hosted on a Linux machine, you may need to use the `-e des-cbc-crc` option to the **`ipa-getkeytab`** command for any nfs/<FQDN> service keytabs you want to set up, both on the server and on all clients. This instructs the KDC to generate only DES keys.

   c. Copy the keytab from the server to the client.

      ```
      # scp /tmp/krb5.keytab root@solarisipaclient.example.com:/tmp/krb5.keytab
      ```

3. On the IPA client, use the **`ktutil`** command to import the contents into the main host keytab.

   ```
   # ktutil
   ktutil: read_kt /tmp/krb5.keytab
   ktutil: write_kt /etc/krb5/krb5.keytab
   ktutil: q
   ```

The IPA client should now be fully configured to mount `NFS` shares using `Kerberos` credentials.

3.2. Configuring Solaris 9 as an IPA Client

Use the same configuration as that used for `Solaris` 10, but replace the PAM configuration with the following:

```
login auth requisite pam_authtok_get.so.1
login auth sufficient pam_krb5.so.1 use_first_pass
login auth sufficient pam_unix.so.1 use_first_pass
login auth required pam_dhkeys.so.1
login auth required pam_unix_auth.so.1
login auth required pam_dial_auth.so.1
```

3.3. Configuring Solaris 8 as an IPA Client

Use the same configuration as that used for `Solaris` 10, but replace the PAM configuration with the following:

```
login auth sufficient /usr/lib/security/pam_krb5.so
login auth required /usr/lib/security/pam_unix.so use_first_pass
login auth required /usr/lib/security/$ISA/pam_dial_auth.so.1
```

3.4. Testing the Configuration

Use the following tests to ensure that the configuration is working correctly:

kinit

Obtain a `Kerberos` ticket for an IPA user.

`$ kinit ipauser` (provide the password when prompted)

`$ klist` (to verify that you received a ticket)

getent

Run the following commands to ensure that **`getent`** in `Solaris` works with IPA.

`$ getent passwd admin`

`$ getent group ipausers`

Console Login

On the system console, provide an IPA username and associated `Kerberos` password to log in.

NFS v4

Use the following command to test the configuration:

`# mount -F nfs -o vers=4 -o sec=krb5 ipaserver.example.com:/ /data`

3.4.1. Troubleshooting

It is possible that the **`mount`** command will hang, and return the following error:

```
rpc.svcgssd[3366]: ERROR: GSS-API: error in handle_nullreq:
gss_accept_sec_context(): Unspecified GSS failure.
Minor code may provide more information - Unknown code krb5 230
```

If this occurs, try the following:

- Destroy the `Kerberos` cache, as follows:

  ```
  # rm -f /tmp/krb*
  ```

  Warning

  Be aware that this will also remove the administrator and user credentials cache, and any other unrelated credentials cache.

- Obtain a new keytab for the `NFS` service using `-e des-cbc-crc` for the IPA client.

- Obtain a new keytab for the `NFS` service principal with `-e des-cbc-crc` for the IPA server.

Configuring AIX as an IPA Client

This chapter describes how to configure AIX as an IPA client. Refer to the IPA *Release Notes* for the currently supported versions of AIX.

Before starting the IPA installation, update your system with all the latest packages.

> **Note**
>
> The IPA client installation process requires that an IPA server already exist.
>
> Many of the following procedures and instructions use example host names, domain names, and realm names for illustration purposes. You need to replace these example names with those that apply to your own deployment.

4.1. Prerequisites

Before you begin the configuration, ensure that the following software is installed and up to date. This can be installed from your AIX media:

- v5.3 OS
- v5.3 Updates
- krb5 client packages
- openssh
- wget
- bash
- krb5 server
- ldap.client
- openssl
- modcrypt.base (for gssd)

4.2. Configuring Client Authentication

Before you begin the following procedures, ensure that `NTP` is correctly configured and enabled, and that time is synchronized between the client and the IPA master.

The `Kerberos` configuration includes specifying the realm and domain details, and default ticket attributes. Forwardable tickets are configured by default, which facilitates connection to the administration interface from any operating system, and also provides for auditing of administration operations.

Procedure 4.1. To configure the AIX client machine:

1. Configure the krb5 client settings as follows:

   ```
   # mkkrb5clnt -r EXAMPLE.COM -d example.com -c ipaclient.example.com -s
   ipaserver.example.com
   ```

2. Get a Kerberos ticket:

   ```
   # kinit admin
   ```

3. Configure the LDAP client settings as follows:

   ```
   # mksecldap -c -h ipaserver.example.com -d cn=accounts,dc=example,dc=com
   -a uid=nss,cn=sysaccounts,cn=etc,dc=example,dc=com -p secret
   ```

4. In the **`/etc/security/ldap`** directory, create the following map files:

   - IPAuser.map

     ```
     #IPAuser.map file
     keyobjectclass SEC_CHAR posixaccount s

     # The following attributes are required by AIX to be functional
     username SEC_CHAR uid s
     id SEC_INT uidnumber s
     pgrp SEC_CHAR gidnumber s
     home SEC_CHAR homedirectory s
     shell SEC_CHAR loginshell s
     gecos SEC_CHAR gecos s
     spassword SEC_CHAR userpassword s
     lastupdate SEC_INT shadowlastchange s
     ```

   - IPAgroup.map

     ```
     #IPAgroup.map file
     groupname SEC_CHAR cn s
     id SEC_INT gidNumber s
     users SEC_LIST member m
     ```

5. Modify the **`/etc/security/ldap/ldap.cfg`** file as follows. Remember to specify your own REALM and basedn values.

   ```
   userbasedn:cn=users,cn=accounts,dc=example,dc=com
   groupbasedn:cn=groups,cn=accounts,dc=example,dc=com

   userattrmappath:/etc/security/ldap/IPAuser.map
   groupattrmappath:/etc/security/ldap/IPAgroup.map

   userclasses:posixaccount
   ```

6. Start the LDAP client daemon:

   ```
   # start-secldapclntd
   ```

7. Test the LDAP client connection to the IPA server:

   ```
   # lsldap -a passwd
   ```

8. Add the following sections to the **/usr/lib/security/methods.cfg** file to configure the system login to use Kerberos and LDAP:

   ```
   KRB5A:
   program = /usr/lib/security/KRB5A
   program_64 = /usr/lib/security/KRB5A_64
   options = authonly

   LDAP:
   program = /usr/lib/security/LDAP
   program_64 =/usr/lib/security/LDAP64

   KRB5ALDAP:
   options = auth=KRB5A,db=LDAP
   ```

9. Edit the **/etc/security/user** file, and modify the "default" section as follows:

   ```
   SYSTEM = "KRB5ALDAP"
   registry = LDAP
   ```

4.3. Configuring Client SSH Access

You can also configure the IPA client to accept incoming SSH requests and authenticate with the user's Kerberos credentials. After configuring the IPA client, use the following procedure to configure the IPA client for SSH connections. Remember to replace the example host and domain names with your own host and domain name.

Procedure 4.2. To configure an AIX IPA client for incoming SSH connections:

1. SSH syslog configuration:

   ```
   auth.info /var/log/sshd.log
   auth.info       /var/log/sshd.log
   auth.crit       /var/log/sshd.log
   auth.warn       /var/log/sshd.log
   auth.notice     /var/log/sshd.log
   auth.err        /var/log/sshd.log
   ```

2. SSH logging configuration:

   ```
   SyslogFacility AUTH
   LogLevel INFO
   ```

3. Configure `sshd` for `GSSAPI` (**`/etc/ssh/sshd_config`**)

   ```
   # GSSAPI options
   GSSAPIAuthentication yes
   #GSSAPICleanupCredentials yes
   ```

4. Restart `sshd`:

   `# stopsrc -s sshd`

   `# startsrc -s sshd`

5. Restart `syslogd`:

   `# stopsrc -s syslogd`

   `# startsrc -s syslogd`

6. The *ipa-admintools* package is not available for AIX. Consequently, you need to perform the following steps on the IPA server.

   a. Add a `host` service principal for the client.

      `# ipa-addservice host/ipaclient.example.com`

   b. Retrieve the `host` keytab.

      `# ipa-getkeytab -s ipaserver -p host/ipaclient.example.com -k /tmp/krb5.keytab -e des-cbc-crc`

   c. Copy the keytab from the server to the client.

      `# scp /tmp/krb5.keytab root@ipaclient.example.com:/tmp/krb5.keytab`

7. On the IPA client, use the **`ktutil`** command to import the contents into the main host keytab.

   ```
   # ktutil
   ktutil: read_kt /tmp/krb5.keytab
   ktutil: write_kt /etc/krb5/krb5.keytab
   ktutil: q
   ```

8. Add a user that is only used for authentication. (This can be substituted with krb5 auth if that works from the ldap client). Otherwise go to the IPA server and use **`ldapmodify`**, bind as `Directory Manager` and create this user.

   ```
   dn: uid=nss,cn=sysaccounts,cn=etc,dc=example,dc=com
   objectClass: account
   objectClass: simplesecurityobject
   objectClass: top
   uid: nss
   userPassword: Your own shared password here
   ```

9. On the IPA server, get a ticket for the `admin` user.

   ```
   # kinit admin
   ```

You should be able to log in as `admin` using `SSH` without providing a password.

```
# ssh admin@ipaclient.example.com
```

4.4. Testing System Login

After you have completed the steps in *Section 4.2, “Configuring Client Authentication”* and *Section 4.3, “Configuring Client SSH Access”*, you should be able to log in as an IPA user on the AIX machine. Use the following tests to ensure that the configuration is working correctly:

On the system console, log in as an IPA user. After you have logged in, open a shell and run the following command:

`$ id` (ensure that the user IDs and group IDs are correct)

If this test fails, refer to the Troubleshooting section in the *Administration Guide* for information on how to locate any problems.

Note

By default, the `admin` user is given **`/bin/bash`** as the shell to use and **`/home/admin`** as the home directory. You may need to install bash (or link **`sh`** to **`/bin/bash`** or modify `admin` to use **`/bin/sh`** or a shell available in all of your systems) to be able to log in.

Configuring HP-UX as an IPA Client

This chapter describes how to configure HP-UX as an IPA client. It also includes some verification tests to ensure that the configuration is working correctly. Refer to the IPA *Release Notes* for the currently supported versions of HP-UX.

Before starting the IPA installation, ensure that you update your system with all the latest packages.

To install an HP-UX client you need administrator privileges in the form of the Directory Manager password. There is no other way to perform the installation.

> **Note**
>
> The IPA client installation process requires that an IPA server already exist.
>
> Many of the following procedures and instructions use example host names, domain names, and realm names for illustration purposes. You need to replace these example names with those that apply to your own deployment.

Configuring NTP

Before proceeding with the following configuration steps, ensure that `NTP` is correctly configured and enabled, and that time is synchronized between the client and the IPA server.

5.1. Configuring LDAP Authentication

Procedure 5.1. To configure LDAP client authentication:

1. Install the ldapux client on the HP-UX 11.23 machine.

   ```
   # swinstall -s J4269AA_B.04.15.01_HP-UX_B.11.23_IA_PA.depot
   ```

2. Change to the configuration directory and run the setup script.

   ```
   # cd /opt/ldapux/config/
   ```

   ```
   # ./setup
   ```

   Note

   You only need to perform this configuration on the first HP-UX client. All further configurations only need to know where the LDAP profile is stored. All clients will then use the same configuration.

   The HP-UX guide for this procedure is located at *http://docs.hp.com/en/J4269-90075/ch02s07.html*

   The following is a sample output from running the above script:

   ```
   Would you like to continue with the setup? [Yes]
   Select which Directory Server you want to connect to ? [RedHat
    Directory]
   Directory server host ? [ipaserver.example.com]
   Directory Server port number [389]
   Would you like to extend the printer schema in this directory server?
    [No]
   Would you like to install PublicKey schema in this directory server?
    [No]
   Would you like to install the new automount schema ? [No]
   Profile Entry DN: [cn=ldapuxprofile,cn=etc,dc=example,dc=com]
   User DN [cn=Directory Manager]
   Password ? [Directory Manager's Password]
   Authentication method ? [ SIMPLE ]
   Enter the number of the hosts you want to specify [1]
   Default Base DN ? [dc=example,dc=com]
   Accept remaining defaults ? [n]
   Client binding [Anonymous]
   Bind time limit [5 seconds]
   Search time limit [no limit]
   Do you want client searches of the directory to follow referrals? [Yes]
   Profile TTL [0 = infinite]
   Do you want to remap any of the standard RFC 2307[1] attribute? [Yes]
   Specify the service you want to map? [ 3=Group]
   Specify the attribute you want to map [3 for memberuid ]
   Type the name of the attribute memberuid should be mapped to [member]
   Specify the service you want to map? [ 0 = exit ]
   Do you want to remap any of the standard RFC 2307[2] attribute? [ no this
    time ]
   Do you want to create custom search descriptors? [ No ]
   ```

3. Ensure that the LDAP client daemon is running.

   # ps -ef | grep ldapclientd

   If necessary, use the following command to start the daemon:

   # /opt/ldapux/bin/ldapclientd

4. Run the following commands to ensure that the LDAP client is working:

   # nsquery passwd admin (user should be visible)

   # nsquery group admins (group and user should be visible)

5. Create a new group on the IPA server.

   # ipa-addgroup testgroup

6. Add a test user to the new group created above.

   # ipa-modgroup -a testuser testgroup

7. Run the **nsquery** commands again to validate the new user and group:

   # nsquery passwd testuser (user should be visible)

   # nsquery group testgroup (group and user should be visible)

8. To ensure that the LDAP client daemon starts when the system boots, add the following lines to the **/etc/opt/ldapux/ldapclientd.conf** file:

   ```
   [StartOnBoot]
   enable=yes
   ```

This concludes the LDAP client configuration.

5.2. Configuring Kerberos and PAM

The `Kerberos` and PAM configuration process is completely manual. Sample configuration files are provided for reference, but you need to edit your own system files to reflect your deployment.

5.2.1. Configuring Kerberos

Edit the **/etc/krb5.conf** file to reflect the following example:

```
[libdefaults]
default_realm = EXAMPLE.COM
default_tkt_enctypes = DES-CBC-CRC
default_tgs_enctypes = DES-CBC-CRC
ccache_type = 2

[realms]
EXAMPLE.COM = {
 kpasswd_server = ipaserver.example.com
```

```
 kdc = ipaserver.example.com:88
 admin_server = ipaserver.example.com:749
 default_domain = example.com
 }

[domain_realm]
.example.com = EXAMPLE.COM
example.com = EXAMPLE.COM

[appdefaults]
kinit = {
 forwardable = true
 }
```

The `Kerberos` configuration includes specifying the realm and domain details, and default ticket attributes. Forwardable tickets are configured by default, which facilitates connection to the administration interface from any operating system, and also provides for auditing administration operations.

5.2.2. Configuring PAM

The PAM configuration differs slightly between different versions of `HP-UX`. These configurations are described below.

HP-UX 11i v2

Edit the **`/etc/pam.conf`** file to reflect the following example:

```
#
# PAM configuration
#
# This pam.conf file is intended as an example only.
# see pam.conf(4) for more details

#
#
################################################################
# This sample file will authenticate the user who belongs to #
# either Kerberos or Unix system. Using this configuration file#
# if the user is authenticated through Kerberos then the Unix #
# authentication will not be invoked. However,if the Kerberos #
# authentication fails for the user, then the fallback #
# authentication mechanism PAM-Unix will be invoked to #
# authenticate the user.The assumption is the user is either #
# present in Kerberos or in Unix system. #
# #
# In case, the administrator wants the password for all the #
# users to be synchronous between Kerberos and Unix systems, #
# then the control flag should to be set to "required" for all #
# the entries with use_first_pass option set for pam_unix. #
# If password synchronization is optional then try_first_pass #
# option need to be set for pam_unix, so that the user can #
# login using the appropriate passwords. #
# #
# The module pam_hpsec(5) is stacked as mandatory module above #
# all the modules for making security checks before #
# authentication. #

################################################################
#
#

# Authentication management
#
login auth required libpam_hpsec.so.1
login auth sufficient libpam_krb5.so.1
login auth required libpam_unix.so.1 try_first_pass
su auth required libpam_hpsec.so.1
su auth sufficient libpam_krb5.so.1
su auth required libpam_unix.so.1 try_first_pass
dtlogin auth required libpam_hpsec.so.1
dtlogin auth sufficient libpam_krb5.so.1
dtlogin auth required libpam_unix.so.1 try_first_pass
dtaction auth required libpam_hpsec.so.1
dtaction auth sufficient libpam_krb5.so.1
dtaction auth required libpam_unix.so.1 try_first_pass
ftp auth required libpam_hpsec.so.1
ftp auth sufficient libpam_krb5.so.1
ftp auth required libpam_unix.so.1 try_first_pass
sshd auth required libpam_hpsec.so.1
sshd auth sufficient libpam_krb5.so.1
sshd auth required libpam_unix.so.1 try_first_pass
OTHER auth required libpam_unix.so.1
#

# Account management
#
login account required libpam_hpsec.so.1
login account sufficient libpam_krb5.so.1
login account required libpam_unix.so.1
su account required libpam_hpsec.so.1
su account sufficient libpam_krb5.so.1
su account required libpam_unix.so.1
dtlogin account required libpam_hpsec.so.1
dtlogin account sufficient libpam_krb5.so.1
dtlogin account required libpam_unix.so.1
dtaction account required libpam_hpsec.so.1
dtaction account sufficient libpam_krb5.so.1
dtaction account required libpam_unix.so.1
ftp account required libpam_hpsec.so.1
ftp account sufficient libpam_krb5.so.1
ftp account required libpam_unix.so.1
```

```
sshd account required libpam_hpsec.so.1
sshd account sufficient libpam_krb5.so.1
sshd account required libpam_unix.so.1
OTHER account required libpam_unix.so.1
#

# Session management
#
login session required libpam_hpsec.so.1
login session sufficient libpam_krb5.so.1
login session required libpam_unix.so.1
dtlogin session required libpam_hpsec.so.1
dtlogin session sufficient libpam_krb5.so.1
dtlogin session required libpam_unix.so.1
dtaction session required libpam_hpsec.so.1
dtaction session sufficient libpam_krb5.so.1
dtaction session required libpam_unix.so.1
sshd session required libpam_hpsec.so.1
sshd session sufficient libpam_krb5.so.1
sshd session required libpam_unix.so.1
OTHER session required libpam_unix.so.1
#

# Password management
#
login password required libpam_hpsec.so.1
login password sufficient libpam_krb5.so.1
login password required libpam_unix.so.1
passwd password required libpam_hpsec.so.1
passwd password sufficient libpam_krb5.so.1
passwd password required libpam_unix.so.1
dtlogin password required libpam_hpsec.so.1
dtlogin password sufficient libpam_krb5.so.1
dtlogin password required libpam_unix.so.1
dtaction password required libpam_hpsec.so.1
dtaction password sufficient libpam_krb5.so.1
dtaction password required libpam_unix.so.1
OTHER password required libpam_unix.so.1
```

HP-UX 11i v1

Edit the **`/etc/pam.conf`** file to reflect the following example:

```
#
# PAM configuration
#
# This pam.conf file is intended as an example only.
# see pam.conf(4) for more details
#

################################################################
```

```
# This sample file will authenticate the user who belongs to #
# either Kerberos or Unix system. Using this configuration file#
# if the user is authenticated through Kerberos then the Unix #
# authentication will not be invoked. However,if the Kerberos #
# authentication fails for the user, then the fallback #
# authentication mechanism PAM-Unix will be invoked to #
# authenticate the user.The assumption is the user is either #
# present in Kerberos or in Unix system. #
# #
# In case, the administrator wants the password for all the #
# users to be synchronous between Kerberos and Unix systems, #
# then the control flag should to be set to "required" for all #
# the entries with user_first_pass option set for pam_unix. #
# If password synchronization is optional then try_first_pass #
# option need to be set for pam_unix, so that the user can #
# login using the appropriate passwords. #

################################################################
#

# Authentication management
#
login auth sufficient /usr/lib/security/libpam_krb5.1
login auth required /usr/lib/security/libpam_unix.1 try_first_pass
su auth sufficient /usr/lib/security/libpam_krb5.1
su auth required /usr/lib/security/libpam_unix.1 try_first_pass
dtlogin auth sufficient /usr/lib/security/libpam_krb5.1
dtlogin auth required /usr/lib/security/libpam_unix.1 try_first_pass
dtaction auth sufficient /usr/lib/security/libpam_krb5.1
dtaction auth required /usr/lib/security/libpam_unix.1 try_first_pass
ftp auth sufficient /usr/lib/security/libpam_krb5.1
ftp auth required /usr/lib/security/libpam_unix.1 try_first_pass
OTHER auth required /usr/lib/security/libpam_unix.1
#

# Account management
#
login account sufficient /usr/lib/security/libpam_krb5.1
login account required /usr/lib/security/libpam_unix.1
su account sufficient /usr/lib/security/libpam_krb5.1
su account required /usr/lib/security/libpam_unix.1
dtlogin account sufficient /usr/lib/security/libpam_krb5.1
dtlogin account required /usr/lib/security/libpam_unix.1
dtaction account sufficient /usr/lib/security/libpam_krb5.1
dtaction account required /usr/lib/security/libpam_unix.1
ftp account sufficient /usr/lib/security/libpam_krb5.1
ftp account required /usr/lib/security/libpam_unix.1
OTHER account required /usr/lib/security/libpam_unix.1
#

# Session management
```

```
#
login session sufficient /usr/lib/security/libpam_krb5.1
login session required /usr/lib/security/libpam_unix.1
dtlogin session sufficient /usr/lib/security/libpam_krb5.1
dtlogin session required /usr/lib/security/libpam_unix.1
dtaction session sufficient /usr/lib/security/libpam_krb5.1
dtaction session required /usr/lib/security/libpam_unix.1
OTHER session required /usr/lib/security/libpam_unix.1
#

# Password management
#
login password sufficient /usr/lib/security/libpam_krb5.1
login password required /usr/lib/security/libpam_unix.1
passwd password sufficient /usr/lib/security/libpam_krb5.1
passwd password required /usr/lib/security/libpam_unix.1
dtlogin password sufficient /usr/lib/security/libpam_krb5.1
dtlogin password required /usr/lib/security/libpam_unix.1
dtaction password sufficient /usr/lib/security/libpam_krb5.1
dtaction password required /usr/lib/security/libpam_unix.1
OTHER password required /usr/lib/security/libpam_unix.1
```

5.2.3. Configuring Access Control

On HP-UX systems a PAM module called pam_authz is available which can be used to control login access to the system based on a user's group membership.

Refer to the HP-UX documentation on pam_authz for details on how to configure access control for HP-UX systems: *http://docs.hp.com/en/B3921-60631/pam_authz.5.html*

5.3. Configuring SSH

Before you can use SSH to connect to the IPA server without using a password, you need to install a suitable version of **ssh**, and set up the correct authentication attributes in the SSH configuration file.

Procedure 5.2. To configure SSH access:

1. Ensure that you have version A.05.10.007 or later of **ssh** installed. Navigate to the following URL to download a suitable version:

   ```
   http://software.hp.com/portal/swdepot/displayProductInfo.do?
   productNumber=T1471AA
   ```

2. Make the following changes to the **`/etc/opt/ssh/ssh_config`** file:
   - Remove any "PreferredAuthentications" entries.
   - Add the following three lines:

     ```
     Host *
     	GSSAPIAuthentication yes
     	PreferredAuthentications "gssapi-with-mic,publickey,password"
     ```

     Important

     Ensure that you include the tab character before the "GSSAPIAuthentication" and "PreferredAuthentications" entries, and the double quotes around the "PreferredAuthentications" argument.

3. Remove the **`/etc/krb5.keytab`** file.

4. On the IPA server:

   a. Add a `host` service principal for the `HP-UX` client.

   ```
   # ipa-addservice host/hpuxipaclient.example.com
   ```

   b. Create the `host` keytab file.

   ```
   # ipa-getkeytab -s ipaserver.example.com -p host/
   hpuxipaclient.example.com -k /tmp/krb5.keytab -e des-cbc-crc
   ```

   c. Copy this keytab to the `HP-UX` machine as **`/etc/krb5/krb5.keytab`**.

   ```
   # scp /tmp/krb5.keytab root@hpuxipaclient.example.com:/etc/krb5/
   krb5.keytab
   ```

5.4. Configuring Access Control

`HP-UX` systems provide a PAM module called pam_authz which can be used to control login access to the system based on a user's group membership. Refer to the following `HP-UX` pam_authz documentation for details on how to configure access control for `HP-UX` systems: *http://docs.hp.com/en/B3921-60631/pam_authz.5.html*

The following is a sample **`/etc/opt/ldapux/pam_authz.policy`** file:

```

# pam_authz.policy.template:
#
# An example file that could be copied over to /etc/opt/ldapux/
pam_authz.policy.
# pam_authz.policy is a local policy file that PAM_AUTHZ would use to help
# determine which users would be allowed to login to the local host.
#
# In this template file, by default, the only active access rule is
#     "allow:unix_local_user"
```

```
# All the local users are authorized to login.
#
# The policy file contains one or more access rule. The format of an access
# rule is <action>:<type>:<object>
#
# where   <action> could be "deny", "allow", "status"
#                           "PAM_SUCCESS", "PAM_PERM_DENIED",
 "PAM_MAXTRIES"
#                           "PAM_AUTH_ERR", "PAM_NEW_AUTHTOK_REQD",
#                           "PAM_AUTHTOKEN_REQD, "PAM_CRED_INSUFFICIENT",
#                           "PAM_AUTHINFO_UNAVAIL", "PAM_USER_UNKNOWN"
#                           "PAM_ACCT_EXPIRED", "PAM_AUTHOK_EXPIRED"
#
#                           Note: "status" must use along with "rhds" or
#                           "ads" <type>.
#         <type>   could be "unix_user", "unix_local_user", "unix_group",
#                           "netgroup", ldap_filter", "ldap_group"
#                           "rhds" or "ads"
#
#                           Note: When <type> is set to "rhds" or "ads",
#                           the <action> filed must set to "status".
#         <object> contains search information. For example,
#

deny:unix_group:admins
allow:unix_local_user
```

This configuration will prevent the admin user from logging in, but local UNIX users can still log in.

5.5. Testing the Configuration

Use the following tests to validate the PAM and `Kerberos` configuration:

- On the HP-UX client machine, run **`kinit admin`** and enter the password.

  `# kinit admin`

  `# klist` (to verify that you received a valid ticket)

- From another Linux client machine, attempt to log in using `SSH`.

  `# ssh admin@hpuxipaclient.example.com`

  The `admin` user should be able to log in using `SSH` without being asked for a password.

- On the HP-UX client console, at the login prompt, enter the Administrator's login ID and password. The `admin` user should be able to log in from the console.

Note

By default, the `admin` user is given **`/bin/bash`** as the shell to use and **`/home/admin`** as the home directory. You may need to install bash (or link sh to /bin/bash or modify `admin` to use /bin/sh or a shell available in all of your systems) to be able to log in.

Configuring Macintosh OS X as an IPA Client

This chapter describes how to configure Macintosh OS X as an IPA client. These instructions are specific to Mac OS X 10.4 (Tiger). This version of the OS includes a partial install of the `Kerberos` tools you need by default, especially if you perform an upgrade from 10.1 or 10.2.

Before starting the IPA installation, ensure that you update the system with all the latest packages.

Note

The IPA client installation process requires that an IPA server already exist.

Many of the following procedures and instructions use example host names, domain names, and realm names for illustration purposes. You need to replace these example names with those that apply to your own deployment.

6.1. Configuring Kerberos Authentication

The current version of IPA does not provide for automatic configuration of Macintosh clients. Configuring authentication is a manual process, and is described in the following sections.

6.1.1. Configuring Kerberos

Configuring the Macintosh to use `Kerberos` for authentication with IPA is a two-step process: First, `Kerberos` needs to be correctly installed and configured, and second, the `Kerberos` authentication needs to be enabled.

Procedure 6.1. To configure the Macintosh to use Kerberos for authentication:

1. Ensure that **`/System/Library/CFMSupport/Kerberos`** is version 4.2 or higher. If that directory does not exist or is the wrong version, install the Kerberos Extras support.

2. Launch **/System/Library/Coreservices/Kerberos**

3. From the **Edit** menu, choose **Edit Realms**.

4. On the **Settings** tab, enter the IPA server's `Kerberos` realm (for example, EXAMPLE.COM).

5. On the **Servers** tab, leave two lines, whose hostnames you then need to replace with the IPA server's hostname (for example, ipaserver.example.com):

```
kdc  ipaserver.example.com 88
admin ipaserver.example.com 749
```

6. On the **Domains** tab, replace the existing domains with the IPA server's actual domain (such as example.com):

   ```
   .example.com
   example.com
   ```

7. Click **Make default** to create the necessary configuration file, and then close the `Kerberos` tool.

   This step creates the **`/Library/Preferences/edu.mit.kerberos`** file, and it is recommended that you check this file manually to ensure that it is correct.

   This file should look similar to the following example. Remember to replace the example.com settings with your own IPA server name, `Kerberos` realm and domain details.

   ```
   [domain_realm]
   example.com = EXAMPLE.COM
   .example.com = .EXAMPLE.COM

   [libdefaults]
   default_realm = EXAMPLE.COM
   dns_lookup_realm = true
   dns_lookup_kdc = true
   ticket_lifetime = 24h
   forwardable = yes

   [realms]
   EXAMPLE.COM = {
    admin_server = ipaserver.example.com:749
    default_domain = example.com
    kdc = ipaserver.example.com:88
    }
   ```

The `Kerberos` configuration includes specifying the realm and domain details, and default ticket attributes. Forwardable tickets are configured by default, which facilitates connection to the administration interface from any operating system, and also provides for auditing of administration operations.

6.1.2. Enabling Kerberos Authentication

You now need to modify the **`/private/etc/authorization`** file to allow `Kerberos` authentication.

Procedure 6.2. To enable Kerberos authentication on the Macintosh:

1. Log in as the `admin` user and launch the **/Applications/Utilities/Terminal** application.

2. Change to the **`/private/etc`** directory and make a backup of the existing authorization file.

   ```
   # cd /private/etc
   ```

   ```
   # cp -p authorization authorization_bak
   ```

3. Open the authorization file, and locate the string "system.login.console".

4. Locate the *`dict`* entry below this string, and then locate the *`mechanisms`* entry.

5. Change *`authinternal`* to *`builtin:krb5authnoverify,privileged`*

> **Warning**
>
> Several instances of *`authinternal`* may occur in this file. Ensure that you change the correct instance.

6. Save and close the file.

7. Restart the machine to enable `Kerberos` authentication.

6.2. Configuring LDAP Authorization

These instructions are specific to Mac OS X 10.4 (Tiger).

6.2.1. Creating the LDAP Configuration

Procedure 6.3. To configure the Macintosh for LDAP authorization:

1. Launch **/Applications/Utilities/Directory Access**.

2. On the **Services** tab, clear all check boxes except `LDAPv3` and `Bonjour`.

3. Select the **LDAPv3** entry and click **Configure**.

4. Ensure the **Add DHCP-supplied LDAP servers** check box is not selected.

5. Click the arrow next to the **Show Options** label, and then click **New**.

6. Enter the Server Name (for example, ipaserver.example.com).

7. Clear the **Encrypt using SSL** check box, and then click **Manual**.

8. Enter the Configuration Name (for example, "IPA LDAP").

9. Ensure that the **Enable** check box is selected, and that the **SSL** check box is cleared.

6.2.2. Setting up the LDAP Service Configuration Options

Procedure 6.4. To configure the LDAP service configuration options:

1. Select the newly-created LDAP configuration and then click **Edit**.

2. On the **Connection** tab, specify the following:

   a. Open/close times out in: 10 seconds

   b. Query times out in: 10 seconds

   c. Re-bind attempted in: 10 seconds

   d. Connection idles out in: 1 minute

   e. Clear all check boxes

3. On the **Search & Mappings** tab, specify the following:

   a. Access this LDAP server using: CUSTOM

   b. In the **Record Types and Attributes** panel, select **Default Attribute Types**, and then click **Add**.

   c. Select the **Attribute Types** option, select **RecordName** from the list, and then click **OK**.

   d. Select the newly-added RecordName attribute, and then click **Add** under the **Map to any items in list** panel.

   e. Type "uid" (without the quotes) in the text box. Click outside of the text box to set the value.

4. Add a Users record, as follows:

   a. Under the **Record Types and Attributes** panel, click **Add**.

   b. Select the **Record Types** option, select **Users** from the list, and then click **OK**.

   c. Select the newly-added **Users** record type, and then click **Add** under the **Map to any items in list** panel.

   d. Type "inetOrgPerson" (without the quotes) in the text box. Click outside of the text box to set the value.

   e. In the **Search base** field, type "dc=example,dc=com" (without the quotes), and select the **Search in all subtrees** option.

5. Add attributes to the Users record as appropriate for your deployment. The following is an example of the required procedure.

   a. Under the **Record Types and Attributes** panel, click **Add**.

   b. Select the **Attribute Types** option, and then use `Command`-Click to select the attributes that you want to add. For example, a typical deployment might include the following attributes:

      - AuthenticationAuthority
      - PrimaryGroupID
      - RealName
      - RecordName
      - UniqueID
      - UserShell

   c. Click **OK** to add the selected attributes to the **Users** record.

6. Specify appropriate mappings for the attributes that you just added. For example:

   a. Select the **Authentication Authority** record type, and then click **Add** under the **Map to any items in list** panel.

   b. Type "#;Kerberosv5;;uid;EXAMPLE.COM" (without the quotes) in the text box. Click outside of the text box to set the value.

   c. Use the same procedure to map PrimaryGroupID to gidNumber.

   d. Use the same procedure to map UniqueID to uidNumber.

   e. Continue until all required entries have been mapped, and then click **OK**.

7. Click **OK** finish setting up the LDAP service configuration options.

6.3. Configuring the LDAP Authorization Options

You now need to add the LDAP service to the list of locations used to search for user authentication information.

Procedure 6.5. To add LDAP to the list of locations to search for authentication information:

1. On the **Authentication** tab, change the **Search** value to **Custom path**, and then click **Add**.

2. Select the configuration that you added in the Creating the LDAP Configuration step, and then click **Add**.

3. Click **Apply** to update the LDAP configuration, and then exit the **Directory Access** application.

6.4. Configuring NTP

Procedure 6.6. To configure the Macintosh to use NTP:

- Open the Date&Time utility and point it to `ipaserver.example.com` to automatically set the date and time.

6.5. Accessing the IPA Server Using SSH

After configuring client authentication, you should be able to use SSH to connect to the IPA server without being prompted for a password.

Procedure 6.7. To test for correct SSH connectivity to the IPA server:

1. Obtain a `Kerberos` ticket for the `admin` user.

   ```
   # kinit admin
   ```

2. If you have a valid `Kerberos` ticket, `SSH` should proceed with GSSAPI authentication without asking for a password:

   ```
   # ssh admin@ipaserver.example.com
   ```

6.6. Configuring System Login

Procedure 6.8. To configure the Macintosh for IPA system login:

1. On the Macintosh login window, log in as an IPA user.

2. After you have logged in, open a terminal and run the following commands:

   `$ id` (ensure that the userid and groupid are correct)

   `$ klist` (ensure that you have a valid `Kerberos` ticket)

Note

To open the Terminal application, navigate to **Applications/Utilities/Terminal.app** or use the keyboard shortcut **`Command-Shift-U`**. You can also drag the Terminal icon to the Dock to make it permanently available on your Desktop.

Using Microsoft Windows to Manage IPA

This chapter describes how to use your web browser on various versions of Microsoft `Windows` to manage IPA.

> **Note**
>
> freeIPA 1.2.1 does *not* support Microsoft `Windows` client authentication.

Refer to the *IPA Release Notes* for information on which versions of Microsoft `Windows` support this configuration.

7.1. Configuring Windows XP Pro and Windows 2000 Pro

Procedure 7.1. To configure both XP Pro and 2000 Pro:

1. Download the MIT Kerberos™ 3.x package for `Windows` to a known location, and then run the **`kfw-3.x-exe`** file that you downloaded to start the **MIT Kerberos Installation Wizard**.

2. Read the license agreement and then click **I Agree** to accept the agreement.

3. Ensure you choose to install KfW Client; the other components are optional.

4. Accept the default destination path.

5. Select **Download from web path**, and enter the following URL:

```
http://<your IPA server's fully-qualified domain name>/ipa/config/
```

6. Select **Autostart the Network Identity Manager each time you login to Windows**.

7. Click **Install** to begin the installation. When the installation is complete, click **Finish** to exit the Wizard.

8. Edit the hosts file and add the IPA server. For example:

```
<numerical IP address>     ipaserver.example.com   ipaserver
```

Depending on the version of Windows, the HOSTS file could be located in different directories. For example:

- Windows 2000 Pro: **`C:\WINNT\system32\drivers\etc\`**

- Windows XP Pro: **`C:\WINDOWS\system32\drivers\etc\`**

Configuring Your Browser

Firefox can use your `Kerberos` credentials for authentication, but you need to specify which domains you want to communicate with, and using which attributes. IPA provides a script that automatically configures Firefox on Red Hat Enterprise Linux and Fedora; for other operating systems, you need to configure your browser manually.

Procedure 8.1. To automatically configure Firefox for use with IPA:

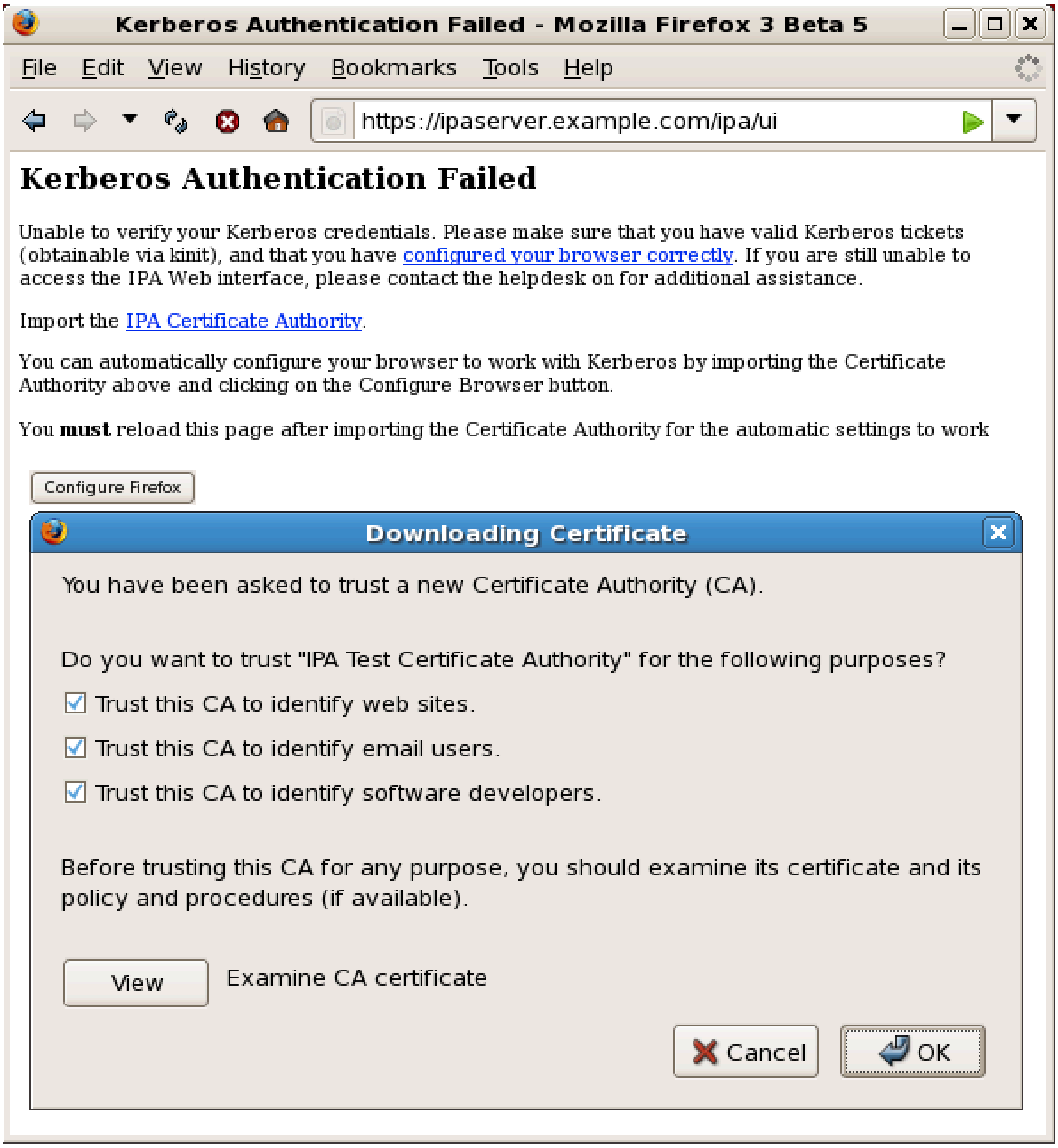
1. Open **Firefox**, and navigate to the IPA server (use the fully-qualified domain name, for example, `http://ipaserver.example.com`). If this is the first time you have attempted to connect to the site, you will see the "Kerberos Authentication Failed" page.

2. Click the **IPA Certificate Authority** link to import the IPA CA into the browser.

3. In the **Downloading Certificate** dialog, select the required trusts and then click **OK**.

4. Press **F5** to reload the web page, and then click **Configure Firefox**.

5. In the **Internet Security** dialog, click **Allow** to enable the IPA script to automatically configure the browser settings.



Kerberos Authentication Failed - Mozilla Firefox 3 Beta 5
File Edit View History Bookmarks Tools Help
https://ipaserver.example.com/ipa/ui

Kerberos Authentication Failed

Unable to verify your Kerberos credentials. Please make sure that you have valid Kerberos tickets (obtainable via kinit), and that you have configured your browser correctly. If you are still unable to access the IPA Web interface, please contact the helpdesk on for additional assistance.

Import the IPA Certificate Authority.

You can automatically configure your browser to work with Kerberos by importing the Certificate Authority above and clicking on the Configure Browser button.

You **must** reload this page after importing the Certificate Authority for the automatic settings to work

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "IPA Test Certificate Authority" for the following purposes?

☑ Trust this CA to identify web sites.

☑ Trust this CA to identify email users.

☑ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Examine CA certificate

Figure 8.1. Importing the IPA CA into Firefox

If you are using an operating system other than Red Hat Enterprise Linux or Fedora, use the following procedure to configure **Firefox**:

Procedure 8.2. To configure Firefox for use with IPA:

1. Open **Firefox**, and type "about:config" in the **Address Bar**.

2. In the **Search** field, type "negotiate".

3. Ensure the following lines reflect your setup. Replace ".example.com" with your own IPA server's domain, including the preceding period (.):

   ```
   network.negotiate-auth.trusted-uris  .example.com
   network.negotiate-auth.delegation-uris  .example.com
   network.negotiate-auth.using-native-gsslib true
   ```

4. - If you are configuring **Firefox** on Microsoft `Windows`, make the following changes instead:

     ```
     network.negotiate-auth.trusted-uris  .example.com
     network.auth.use-sspi false
     ```

5. In **Firefox**, navigate to the IPA server (use the fully-qualified domain name, for example, `http://ipaserver.example.com`). Ensure that there are no `Kerberos` authentication errors, and that you can see and interact with the Web interface.

If you have issues connecting to the IPA server using your web browser, refer to the Troubleshooting section of the *IPA Administration Guide*.

Appendix A. Revision History

Revision 1.2	6 Jan, 2009	David O'Brien `davido@redhat.com`

BZ 474212. Update HP-UX access control doc.
BZ 476060. Update installation procedure for RHEL 5 client packages.
BZ 474253. Document passwordless SSH login restriction for RHEL 3.
BZ 475416. Add client configuration steps for RHEL 2.1 and 3.
BZ 470605. Document SSH access for HP-UX.
BZ 471994. Updates to AIX configuration.
BZ 469995. Updates from Tech Review.

Revision 1.1	4 Nov, 2008	David O'Brien `davido@redhat.com`

BZ 468210. Updated *nss_ldap* requirements for Solaris.
BZ 469790. Updated Web Browser Configuration section.

Revision 1.0	1 July, 2008	David O'Brien `davido@redhat.com`

Created.