



## Contents

<b>1 INTRODUCTION</b> .....	<b>2</b>
1.1 Scope .....	2
1.2 Definition of Terms .....	2
<b>2 SERVER CONFIGURATION</b> .....	<b>3</b>
2.1 Supported Deployment Configurations .....	3
2.1.1 Single AD2008 Domain Controller .....	3
2.1.2 Two Domain Controllers in Trust Relationship .....	4
2.2 The iPrism Active Directory Account .....	6
2.3 Client Active Directory Accounts .....	8
<b>3 IPRISM CONFIGURATION</b> .....	<b>10</b>
3.1 To set iPrism to use the Domain Controller as its NTP server.....	13
3.2 Verify the existence of an A record.....	13
<b>4 CLIENT CONFIGURATION</b> .....	<b>14</b>
4.1 Important Notes.....	14
4.2 Windows Clients .....	14
4.2.1 Internet Explorer on Windows .....	16
4.2.2 Firefox on Windows.....	20
4.3 Mac Clients.....	21
4.3.1 Configuring the Mac.....	21
4.3.2 Joining a Mac to Active Directory 2008 .....	22
4.3.3 Safari on OS X .....	24
4.3.4 Firefox on OS X.....	24
<b>5 KNOWN ISSUES</b> .....	<b>25</b>
5.1 Kerberos Key Mismatch .....	25
5.2 Other Issues .....	25

## 1 Introduction

---

This document is intended to be a comprehensive reference detailing the environments supported when deploying iPrism 6.400 in a Windows® 2008 Active Directory® environment.

### 1.1 Scope

---

The information in this document is limited to the 6.400 version of iPrism, deployed in an environment where the iPrism appliance is to be integrated with a Microsoft Windows® Active Directory 2008 server.

### 1.2 Definition of Terms

---

The terms included in the table below are used throughout this document.

Term/Acronym	Description
AD2003	Microsoft Active Directory 2003
AD2008	Microsoft Active Directory 2008
DNS	Domain Name System: The system by which Internet domain names and addresses are tracked and regulated.

## 2 Server Configuration

---

DNS should be running on the Active Directory Server. To verify this, do the following:

Verify this by choosing *Start → All Programs → Administrative Tools → Services*.

Verify that *DNS Server* has a status of *Started*. The administrator will need to manually create a *DNS A record* for the iPrism if DNS is running on a server other than the Domain Controller.

Ensure that the *Time Skew* (the time difference between the AD2008 server and any client (PC or iPrism)) is less than 5 minutes. If there is a problem, the iPrism may be unable to join the Active Directory domain and clients may not be able to authenticate.

### 2.1 Supported Deployment Configurations

---

To be supported by the iPrism 6.400 software, AD2008 must be deployed in one of the following configurations.

#### 2.1.1 Single AD2008 Domain Controller

In this first scenario, the iPrism is joined directly to a single AD2008 domain controller, allowing the iPrism to authenticate users against that AD2008 domain. Negotiate authentication is supported (Kerberos with a fallback to NTLM) when the following are true:

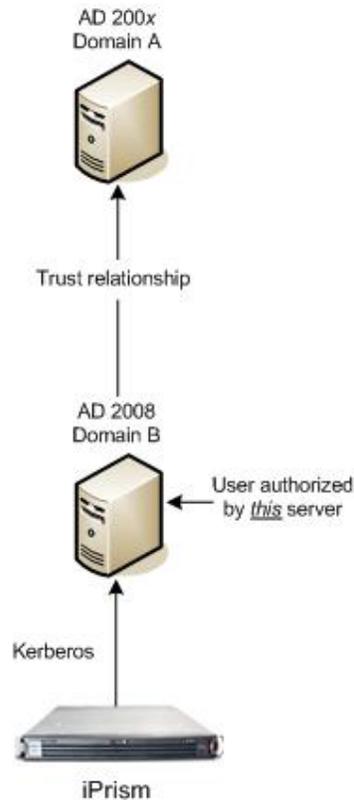
- In any mode where the user is joined to an AD2008 domain,
- The workstation is a member of the domain or any domain trusted by the domain,
- And the user is logged in as a member of the domain or any domain trusted by the domain.

Whether to use Kerberos or NTLM is determined by the user's browser. There is one exception: Internet Explorer 6, when used in Proxy mode, always uses NTLM and refuses Negotiate authentication mode. This is supported by iPrism.

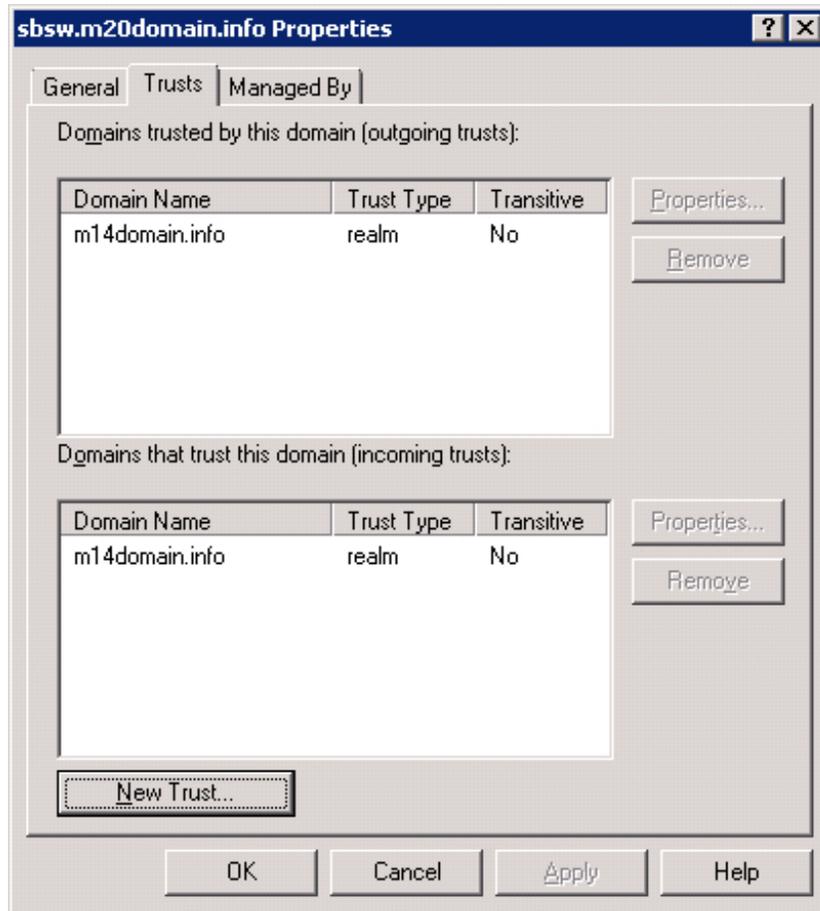


### 2.1.2 Two Domain Controllers in Trust Relationship

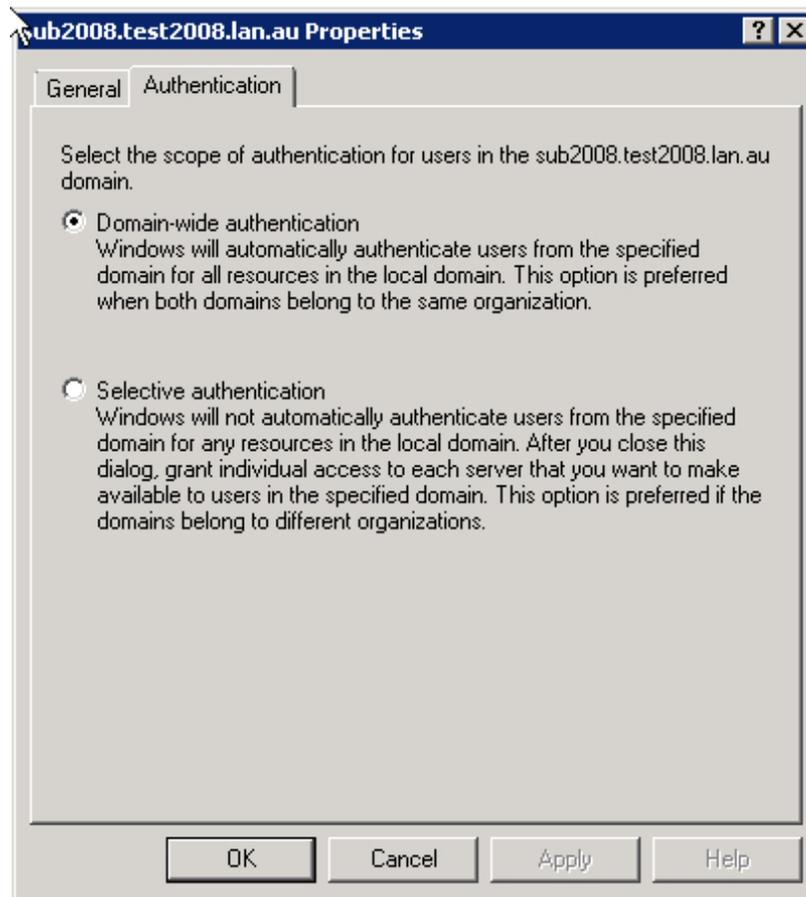
In this second scenario, the iPrism is joined to a domain served by an AD2008 domain controller using Kerberos, and that domain controller has a **two-way** trust relationship with a second AD2008 or AD2003 domain controller. When iPrism is joined to a domain served by an AD2008 domain controller, iPrism users may authenticate in the domain served by the AD2008 domain controller. Users may authenticate in any domain trusted by that domain. To authenticate in a trusted domain, a two-way trust must exist.



The key trust settings are displayed in the following screenshot. Note that the two-way trust results in *external, non-transitive* entries in both the *outgoing trust* and *incoming trust* lists.



Additionally, in the *Properties* for the trust list entries, the authentication is set to *Domain-wide authentication*.



## ***2.2 The iPrism Active Directory Account***

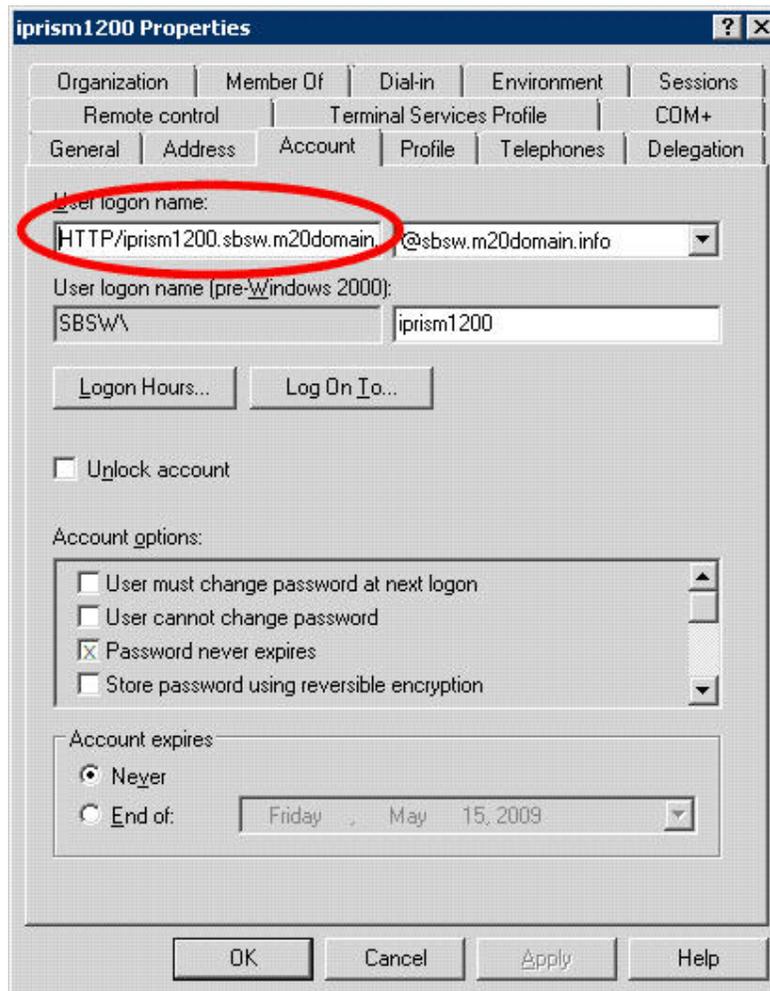
---

An AD2008 user account should be created and have **Password never expires** checked. No other changes should ever be made.

**Important:** **Password never expires** should be checked because if a password expires, a domain-wide authentication failure is likely to occur, particularly if the password is that of the user whose account is used to join the domain.

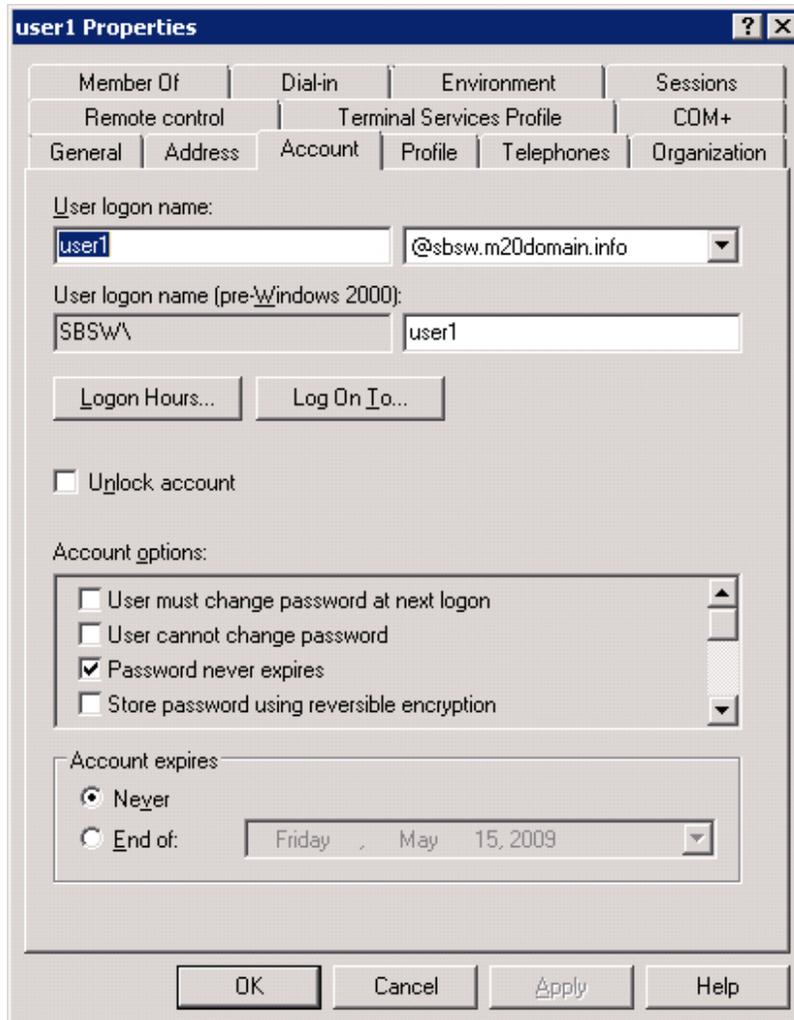
To verify that the account has not been modified, the settings on the **Account** tab can be compared to the correct ones in the following screenshots. Substitute your iPrism account name for *iprism100h* and your own domain for *sbsw.m20domain.info*.

The key information to check on the Account tab is that the *User logon name* is in the format `HTTP/username.domain`:

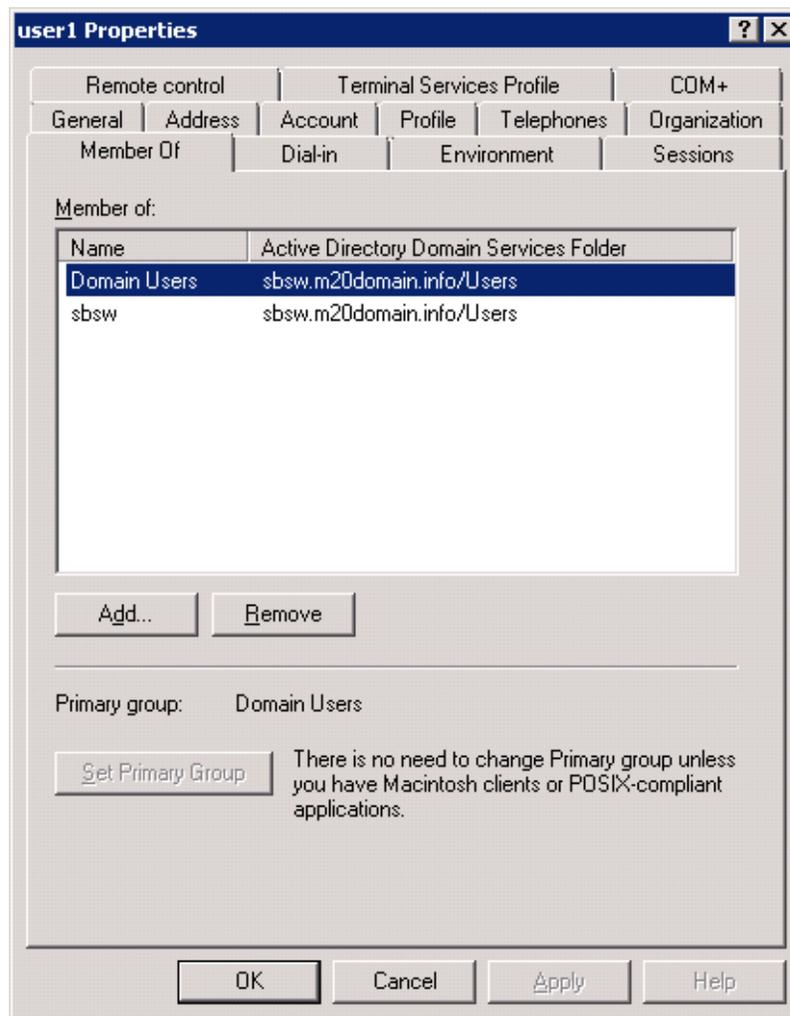


### 2.3 Client Active Directory Accounts

User accounts on the Active Directory for use by the clients themselves can be simple user accounts, as per the following example:



The minimum requirement is that the accounts are members of the *Domain Users* group, as shown in the following example:



### 3 iPrism Configuration

1. From the iPrism home page, select **System Settings**, then **Directory Services**.
2. Click **Configure & Join**.
3. From the **Authentication Mode** dropdown list, choose **Server 2008**.

#### Authentication Mode and Status

Authentication Mode

Server 2008 ▼

#### Domain Settings

<p>NT Domain</p> <div style="border: 1px solid #ccc; padding: 2px;">IPDEV</div> <p>Active Directory Realm</p> <div style="border: 1px solid #ccc; padding: 2px;">ipdev.com</div> <p>Machine Account</p> <div style="border: 1px solid #ccc; padding: 2px; border-color: red;">ipdev.com\ipdev</div> <p>Username</p> <div style="border: 1px solid #ccc; padding: 2px;"></div>	<p>Domain Controller(s)</p> <div style="border: 1px solid #ccc; padding: 2px; min-height: 50px;">ipdev.com</div> <div style="display: flex; justify-content: space-around; margin-top: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #4F81BD; color: white;">Add</div> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #4F81BD; color: white;">Edit</div> <div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #4F81BD; color: white;">Delete</div> </div> <p>Password</p> <div style="border: 1px solid #ccc; padding: 2px;"></div>
---	---

[Advanced Settings](#)

#### Auto-login Redirection Settings - only relevant in Bridge (transparent) mode

DNS

Requires iPrism host entry into all participating network zones.

[Join](#)

[Cancel](#)

4. Your NT Domain, Active Directory Realm, Machine Account, and Domain Controllers will be populated. You can change any of these if necessary.

**Note:** If you change the prepopulated Active Directory Realm, you must use a fully qualified domain name.

If you change the Machine Account, you must specify a unique machine account name for iPrism. (iPrism must establish a machine account on the NT domain.)

**Note:** The account will be created with this name and should be defined so as to not conflict with other machine accounts on the domain. This new account must remain, as created by the Join operation, for the duration of iPrism's participation within the domain. If the account is accidentally removed from the NT server, the Join procedure must be repeated again.

5. Type the username and password of the user account that belongs to the Domain Administrator group in the **User name** and **Password** fields, respectively.

**Important:** The username must be a member of the "Domain Admins" group for the AD 2008 domain.

This account need not be in the same AD domain as the iPrism is joining. However, this account **MUST** have administrative rights in the AD domain that the iPrism is joining. (Permissions may be granted via a trust relationship between domains.)

The only allowable formats are as follows:

```
Username (e.g., jdoe)
NT Domain\Username (e.g., SALES-ABC\jdoe)
Username@ADDomain (e.g., jdoe@sales.abc.com)
```

6. Click **Advanced Settings**.
7. The fields will be prepopulated based on your authentication settings. You can change any of these if necessary:

**Active Directory Server IP Port** (in the example above, 389).

**Search User DN** needs to be a domain user account. The DN can be in Windows 2003/2008 LDAP format or Windows 2003/2008 UPN format (e.g., admin@iprism.abc.com).

**Search User Password** .

**Important:** It is **not recommended** that you change the **Search User DN** or **Search User Password** fields.

The **Search Base** field is prepopulated, and should be set to the root domain object of the AD forest (e.g., DC=sbsw, DC=m20domain, DC=info).

The **Search Mask** field is prepopulated, and should be set to sAMAccountName=%1 (preferably) or userprincipalname=%1

The **Group Attribute** field is prepopulated, and should be set to memberOf. Each node will usually have many attributes of information about the user.

iPrism can run up to two queries to determine a user's profile. If the value in the **Group Attribute** field is a distinguished name, iPrism will perform a second query, searching for the **Group Attribute Name** . This allows the ability to use groups to define profiles, so you will not have to reconfigure individual users. For example:

```
Query for user <CN=joe, DC=stbernard, DC=com> returns the values
memberOf = <CN=group1, DC=stbernard, DC=com>
memberOf = <CN=group2, DC=stbernard, DC=com>
```

The iPrism client will then query each 'memberOf' group until it finds a valid attribute. Since there is no mapping yet, the first valid attribute is used. iPrism can also just retrieve a single attribute to use as the name of an access profile on iPrism. This will then be associated with the user for access privileges. If you want to use this feature, configure your AD08 server to provide such information under a specific attribute name, and list that name in the **Group Attribute Name** field.

8. If a Group Attribute Name is defined, iPrism will proceed as follows:
  1. Authenticate the user using provided credentials
  2. Look up the value of the (primary) attribute for the user
  3. If the attribute is a DN, look up this DN
  4. Search for the secondary (SubQuery) attribute of this DN
  5. Use the value of the secondary attribute as the iPrism filtering profile name

**Note :** For multi-valued attributes, the first valid match (meaning the value maps to an existing iPrism profile) will be used.

9. Select an **Encryption Type** from the dropdown list. The following Encryption Types are available:
  - TLS/SSL
  - TLS
  - SSL
  - None

**Note :** Unless the AD Server has been set up with a server certificate, select **None** .

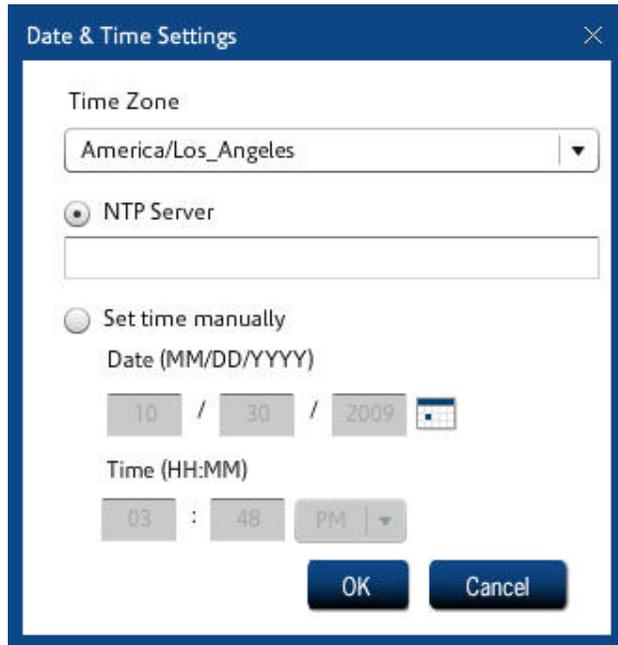
10. Click **OK** .
11. Bridge (transparent) mode only : **Auto-Login Redirection Settings**.  
When using Server 2008, DNS is the only option available for Auto-Login redirection settings. DNS redirection is required for Auto-Login, because iPrism uses its fully qualified domain name to generate Kerberos keys during Auto-Login. The name iPrism uses for redirection must agree with this name. Setting DNS redirection causes the iPrism to use the same name for both its Kerberos keys and for redirection. For more information about how DNS works with Auto-Login, see the iPrism Knowledgebase article "How do I resolve iPrism's IP address using DNS?"
12. If your settings are correct, click **Join** in the Join Domain Settings frame .  
**Important:** This may take a few minutes. If there is a problem, you will receive an error message; as long as the progress bar is working, do not click **Cancel** or assume there is a problem.
13. Click **Yes** to confirm.
14. Save your configuration by clicking **Save** .
15. If all settings are correct and the join was successful, under **Current Authentication Mode** , you will see **AD200x - Joined** .
16. Set up your clients' browsers. For instructions on specific browsers, refer to the following articles in the Knowledgebase:
  - "Configuring IE for proxy mode Auto-Login"
  - "Configuring IE for transparent mode Auto-Login"
  - "Configuring Firefox"

**Important:** Users must proxy to iPrism's fully qualified domain name, not the IP address.

### ***3.1 To set iPrism to use the Domain Controller as its NTP server***

---

1. From the iPrism home page, select **System Settings**, then **System Preferences**.
2. In the Current Date & Time frame, click **Set**.
3. In the NTP Server field, type the IP address of the server that handles NTP requests.



### ***3.2 Verify the existence of an A record***

---

Verify that the iPrism has a valid *A record* listed in the DNS server used by the clients.  
**(Note:** The required A record is for iPrism.)

- If the DNS is not running on the Domain Controller, then a manual *A record* will need to be created on the DNS Server. For instructions on how to do this, see the iPrism Knowledgebase article "How do I setup a DNS A-record for iPrism?", available at [www.stbernard.com/products/support/iprism/help/iprism.htm](http://www.stbernard.com/products/support/iprism/help/iprism.htm)

**Note:** If the machine isn't joined to the same domain, you will be prompted and required to enter your credentials.

## 4 Client Configuration

---

Ensure that the *Time Skew* (the time difference between the AD2008 server and any client (PC or iPrism)) is less than 5 minutes. If there is a problem, the iPrism may be unable to join Active Directory and clients may not be able to authenticate. If there is a problem, follow the steps on page 13 to set up the Domain Controller as your NTP server.

### 4.1 Important Notes

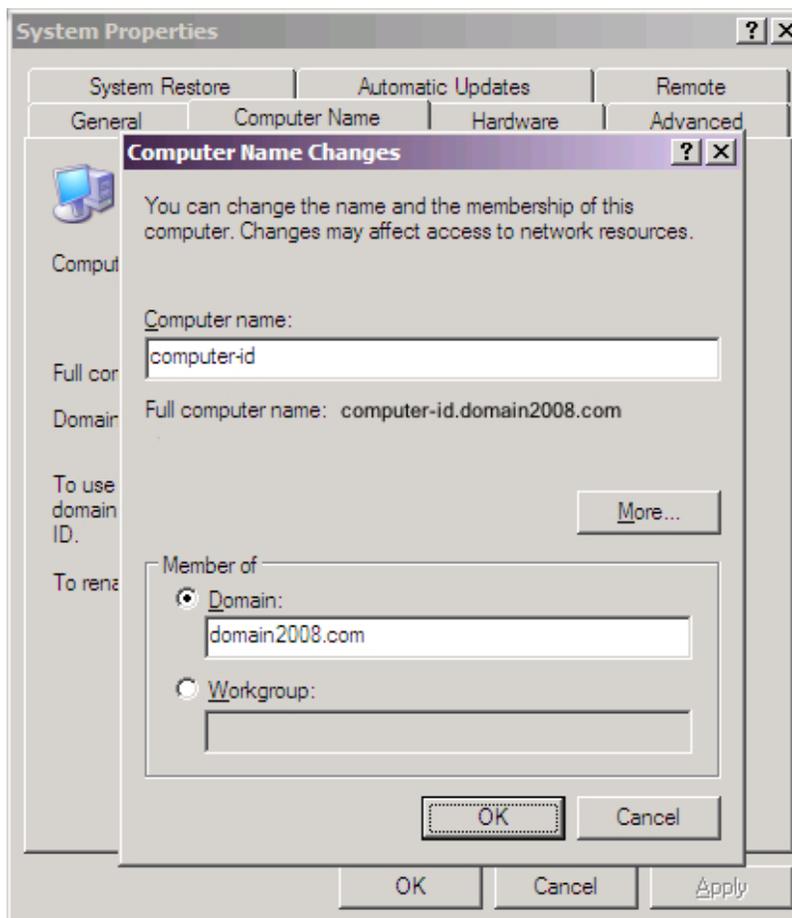
---

- If you are using iPrism in proxy mode, the Local Intranet Zone setting is not required.
- If you are using iPrism in bridge (transparent) mode, the proxy setting is not required.

### 4.2 Windows Clients

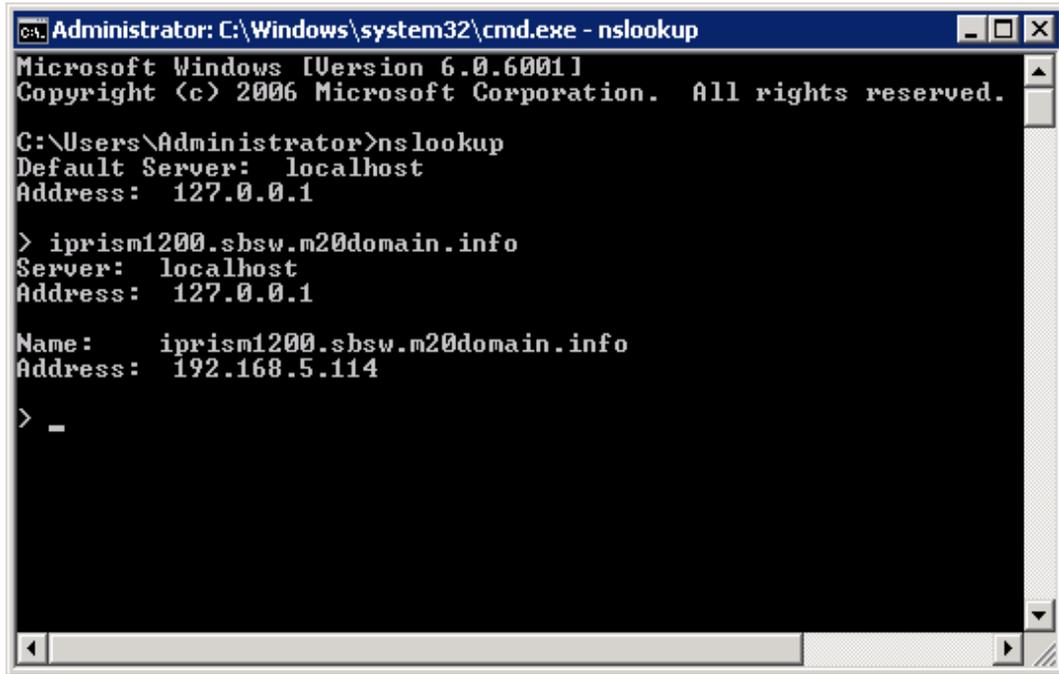
---

The Client PC must be joined to the same domain as the iPrism.



The Client must be logged in with a user account that exists on the same domain as the iPrism.

Ensure that the client PC can resolve the iPrism host name via the *nslookup* command.



```
Administrator: C:\Windows\system32\cmd.exe - nslookup
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup
Default Server: localhost
Address: 127.0.0.1

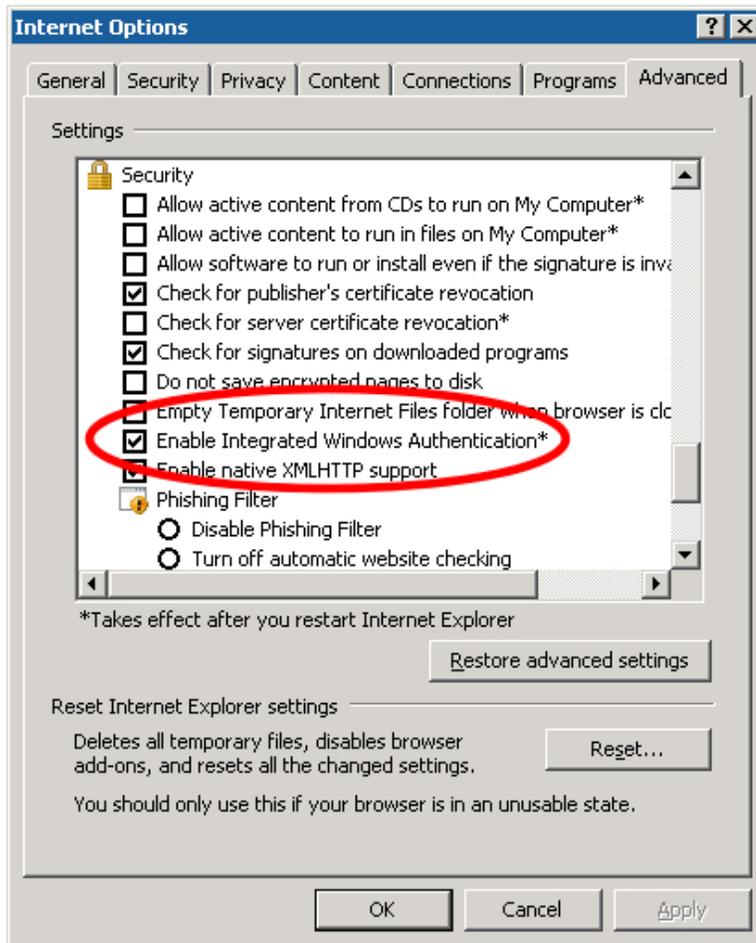
> iprism1200.sbsw.m20domain.info
Server: localhost
Address: 127.0.0.1

Name: iprism1200.sbsw.m20domain.info
Address: 192.168.5.114

> _
```

#### 4.2.1 Internet Explorer on Windows

Ensure that *Integrated Windows Authentication* is enabled on the client:

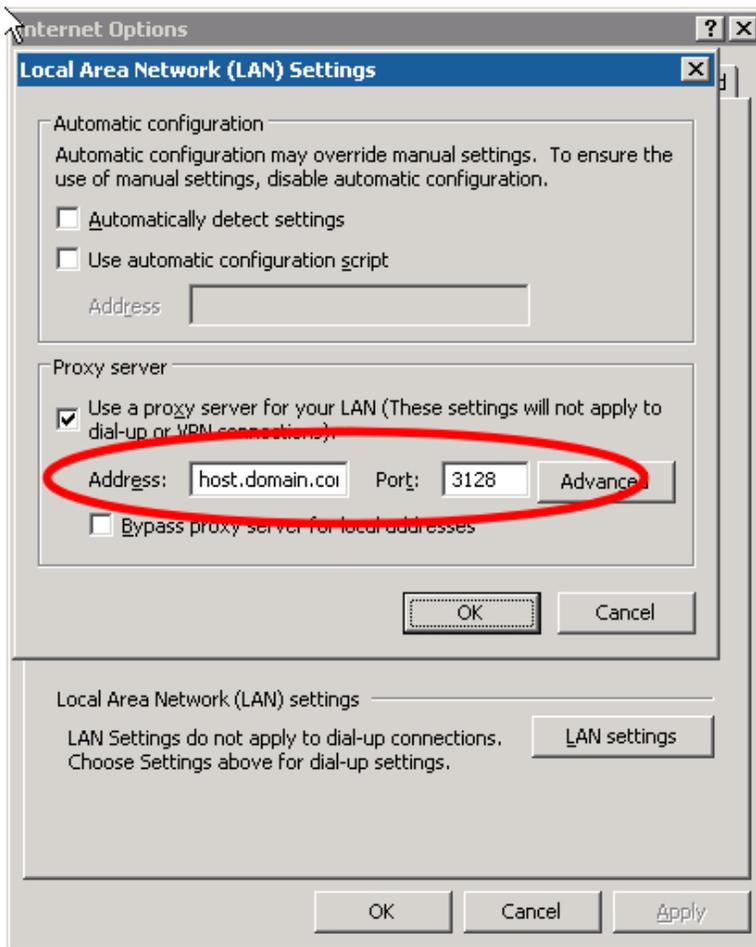


The above setting corresponds to the following registry key:  
 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet  
 Settings\EnableNegotiate = DWORD:1 (for Kerberos).

**Important:**

- Internet Explorer 6 does not support Kerberos in proxy mode (IE 6 only supports Kerberos in bridge (transparent) mode), so ensure that at least version 7 of IE is being used on any client machines that are going to proxy through iPrism.
- Internet Explorer 7 cannot be used on Windows 2000 clients; customers who require proxy support on Windows 2000 must use Firefox.

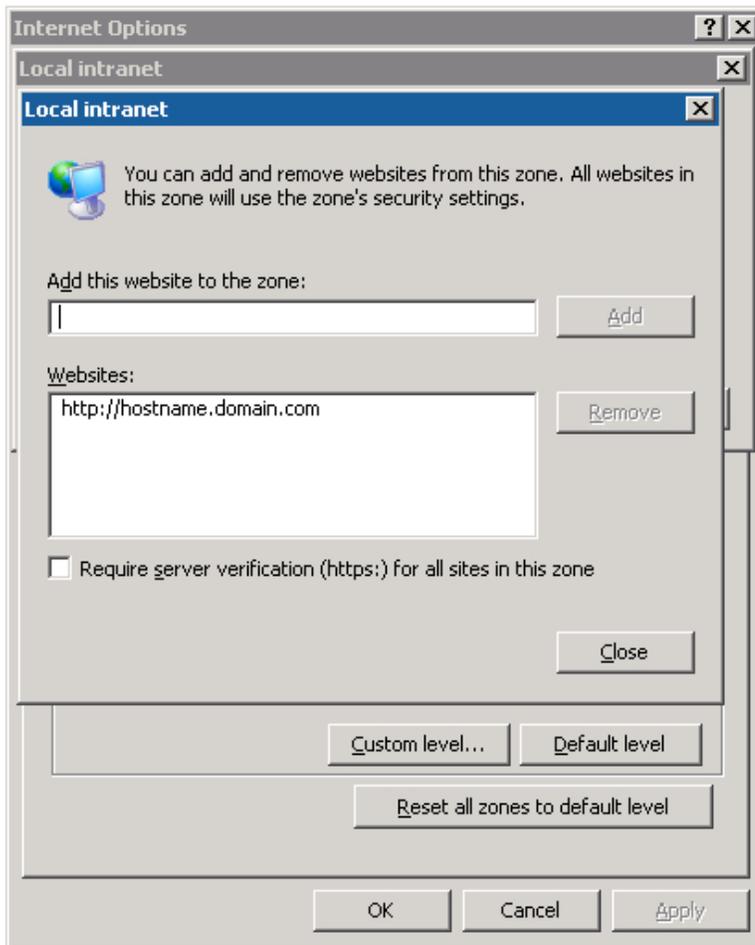
In Internet Explorer, specify the fully qualified domain name of the iPrism<sup>1</sup> in the **Proxy server** section of the **Local Area Network (LAN) Settings**:



<sup>1</sup> If you are using iPrism in proxy mode, you can specify *either* the proxy server's fully qualified domain name or its IP address here. However, if you are using iPrism in bridge (transparent) mode, you must use the fully qualified domain name. IP address cannot be used.

In Internet Explorer, add the fully qualified domain name of the iPrism to the **Local intranet** zone as follows:

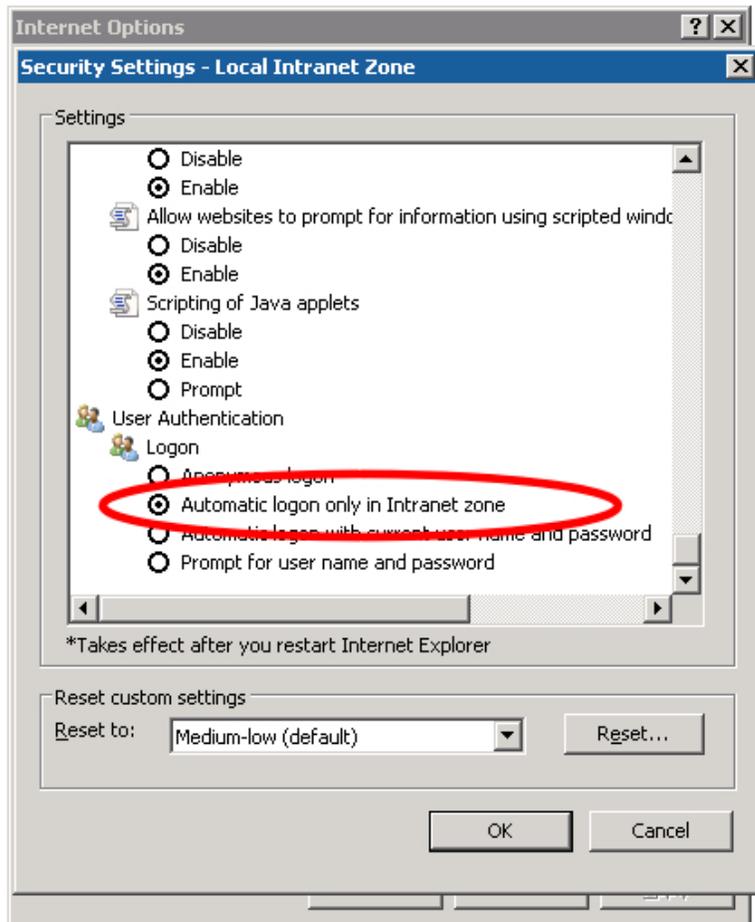
- Select **Tools** → **Internet Options** → **Security** → **Local Intranet** → **Sites** → **Advanced**.
- Type the fully qualified domain name.
- Click **Add**.



Internet Explorer must be configured for Integrated Authentication.

Verify this as follows:

- Select **Tools** → **Internet Options** → **Security** → **Local Intranet** → **Custom Level**.
- Scroll down to the bottom of the list and ensure **Automatic logon only in Intranet zone** is selected.



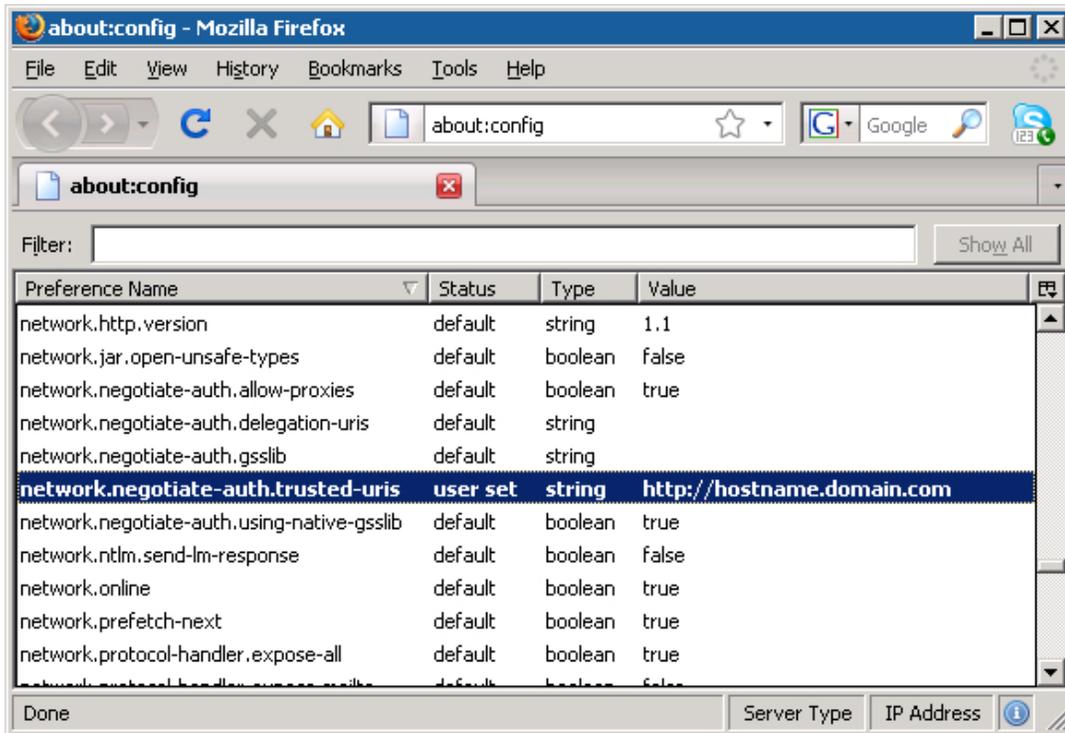
#### 4.2.2 Firefox on Windows

For clients who are using Firefox as their browser:

- Type *about:config* in the address bar.

Search for the key *network.negotiate-auth.trusted-uris* .

Set the value to the fully qualified domain name of the iPrism.



### 4.3 Mac Clients

**Important Note:** Auto-Login is only supported on OS X version 10.5.

Mac clients must be configured and then joined to the same domain as the iPrism. To do this, complete the following instructions.

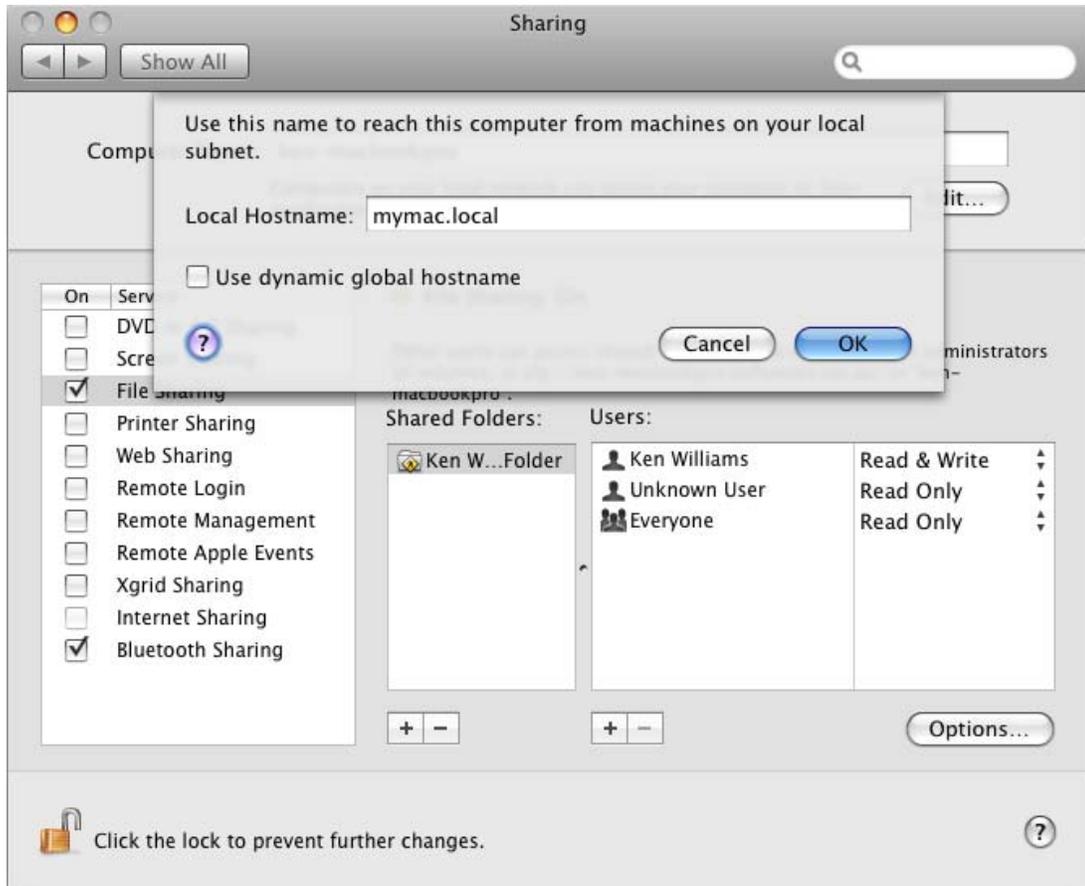
#### 4.3.1 Configuring the Mac

- Set the Mac's DNS (*System Preferences* → *Network* → *Advanced* → *DNS*) to point to the Domain Controller (if the Domain Controller is also the DNS server) or to a DNS server that can resolve the Domain Controller's name.
- Add the domain name to the search suffixes.



Via *System Preferences* → *Sharing*, set the Mac's hostname to a reasonable value (a valid DNS hostname of 15 characters or less).

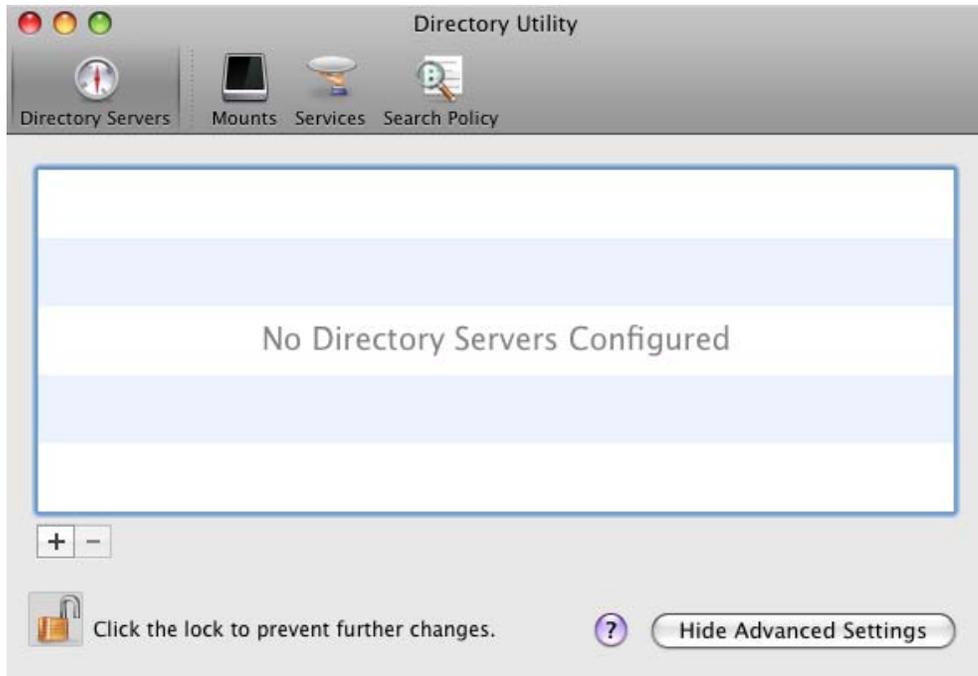
Under *Computer Name*, click *Edit...* to edit the hostname. Leave the default suffix *.info* (or *.local*) alone if it is there; it will be ignored.



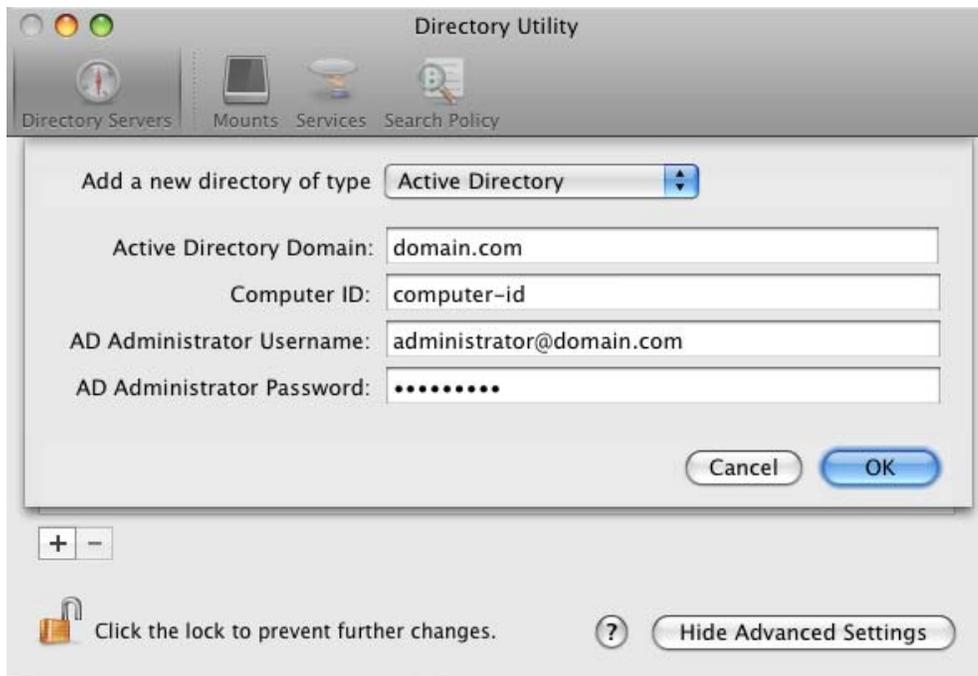
Set the Mac's hostname in your DNS server. It's most convenient if your DNS server is also your Domain Controller, but it doesn't have to be.

#### 4.3.2 *Joining a Mac to Active Directory 2008*

- Open the Applications folder and browse to the Utilities folder.
- From here, start up the *Directory Utility* application.



Click the + sign to add a directory. When that dialog opens, select *Active Directory* and you will see the following dialog:



Credentials must be provided in the newer user@domain.tld form. Once joined, you will see the directory listed in the Directory Utility.

When logging into the Mac, ensure that you select a user account that exists on the same domain as the iPrism.

### 4.3.3 Safari on OS X

Launch Safari and surf to a web site. If the client IP address has been configured in the iPrism for Auto-Login, a popup dialog will appear asking for your Kerberos password and a checkbox asking whether you want to add it to your keychain.

**Important Note:** Auto-Login is only supported on OS X version 10.5.

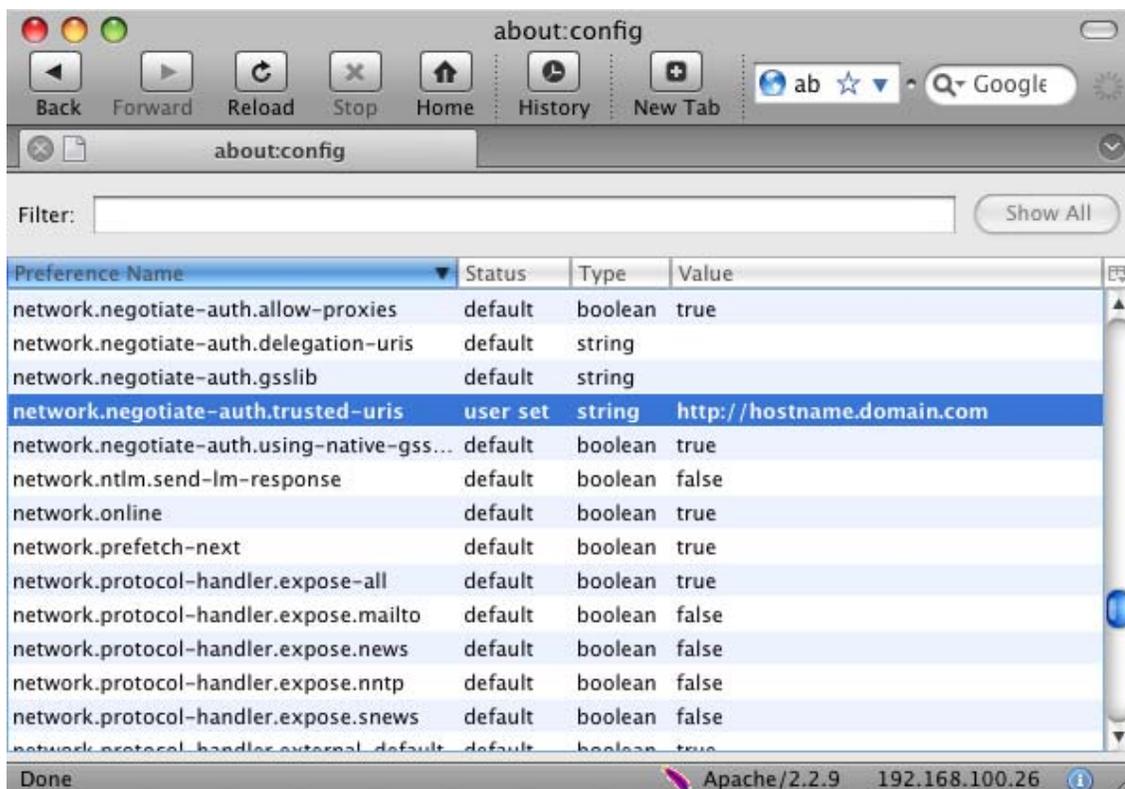
- Type your password.
- Check the box if you want to add the password to your keychain.

Safari should connect. If you add your password to your keychain, you should not be prompted again.

### 4.3.4 Firefox on OS X

For clients who are using Firefox as their browser:

- Type *about:config* in the address bar.
- Search for the key *network.negotiate-auth.trusted-uris* .
- Set the value to the fully qualified domain name of the iPrism.



## 5 Known Issues

---

The following known issues exist in the iPrism 6.3/AD2008 environment.

### 5.1 Kerberos Key Mismatch

---

In some cases, we are seeing a Kerberos key mismatch between clients and the Active Directory server. This problem manifests itself by prompting the client with a login dialog box in the browser (as per Basic authentication) even when Auto-Login has been configured for that client. Logging in with valid credentials allows the client to proceed.

Active Directory does not maintain keys that it has generated previously for clients, but rather only the current key that will be given out; once generated, they are gone and there is no way to get at them. Hence the general recommendation is to only ever touch the user account being used for Kerberos from a single place (e.g., by using the *ktpass* command).

There does not appear to be a way to force a client to get rid of its key. It will continue using the "host" key no matter how many times login fails. It will, however, re-fetch the "HTTP" key each time it tries to do a manual login, which is why even when Auto Login fails, manual login still works.

**The only way to ensure this doesn't happen is to educate users that they should not, under any circumstances, change the password on the iPrism Active Directory account.**

If for some reason the password is changed, then rejoining the domain should fix it going forward (since it will update the key to something that the iPrism will have in its *keytab*).

However, any clients that have fetched the key in the meantime will be forced to manually login until such time as they log out (and hence flush their Kerberos cache).

### 5.2 Other Issues

---

- The Administrator will need to **Save & Exit** the iPrism System Configuration tool after joining the AD2008 server and before mapping groups.

If you map a group before doing a **Save & Exit** and logging back into iPrism, the group mapping will be saved but cannot be checked or used until after you have completed a **Save & Exit**.

**Note:** Policy Mapping does not currently work for nested groups.

- Regarding the Active Directory Local Policy Setting *Deny access to this computer from the network*, this security setting determines which users are prevented from accessing a computer over the network. This policy setting supersedes the *Access this computer from the network* policy setting if a user account is subject to both policies. As a result, if it is enabled with domain users, Internet access is unfiltered when Auto-Login is used.



# Active Directory 2008 Implementation

Version 6.410

©2001-2010 St. Bernard Software, Inc. All rights reserved.  
The St. Bernard Software logo, iPrism and iGuard are trademarks of St. Bernard Software Inc.  
All other trademarks and registered trademarks are hereby acknowledged.



## Corporate Office

15015 Avenue of Science  
San Diego, CA 92128

Main Phone: 858-676-2277

Toll Free: 800-782-3762

Fax: 858-676-2299

Email: [info@stbernard.com](mailto:info@stbernard.com)

Web: [www.stbernard.com](http://www.stbernard.com)