Contents

1 INTRODUCTION ............................................................................................................. 2
  1.1 Scope.......................................................................................................................... 2
  1.2 Definition of Terms..................................................................................................... 2

2 SERVER CONFIGURATION ............................................................................................ 3
  2.1 Supported Deployment Configurations................................................................. 3
  2.1.1 Single AD2008 Domain Controller ................................................................. 3
  2.1.2 Two Domain Controllers in Trust Relationship ............................................... 3
  2.2 The iPrism Active Directory Account ................................................................. 6
  2.3 Client Active Directory Accounts ......................................................................... 8

3 IPRISM CONFIGURATION ............................................................................................ 10
  3.1 To set iPrism to use the Domain Controller as its NTP server ......................... 13

4 CLIENT CONFIGURATION ............................................................................................. 15
  4.1 Important Notes.......................................................................................................... 15
  4.2 Windows Clients ........................................................................................................ 15
    4.2.1 Internet Explorer on Windows ......................................................................... 17
    4.2.2 Firefox on Windows .......................................................................................... 21
  4.3 Mac Clients ................................................................................................................ 22
    4.3.1 Configuring the Mac .......................................................................................... 22
    4.3.2 Joining a Mac to Active Directory 2008 ....................................................... 23
    4.3.3 Safari on OS X .................................................................................................. 25
    4.3.4 Firefox on OS X ............................................................................................... 25

5 KNOWN ISSUES ............................................................................................................. 26
  5.1 Kerberos Key Mismatch ............................................................................................ 26
  5.2 Other Issues ............................................................................................................... 26
1 Introduction

This document is intended to be a comprehensive reference detailing the environments supported when deploying iPrism 6.300 in a Windows® 2008 Active Directory® environment.

1.1 Scope

The information in this document is limited to the 6.300 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.

<table>
<thead>
<tr>
<th>Term/Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD2003</td>
<td>Microsoft Active Directory 2003</td>
</tr>
<tr>
<td>AD2008</td>
<td>Microsoft Active Directory 2008</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System: The system by which Internet domain names and addresses are tracked and regulated.</td>
</tr>
</tbody>
</table>
2 Server Configuration

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

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

2. 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.

3. 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 6.300 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 an AD2008 domain controller using Kerberos, and that domain controller has a two-way trust relationship with a second...
AD2008 or AD2003 domain controller. iPrism users can only be authenticated against the AD2008 controller to which the iPrism is directly joined.

Note: One-way trusts are supported when iPrism is joined to the trusting domain and the users are logged in to trusted domains. One-way trusts are supported when the domain of the iPrism has an outgoing trust to the user’s domain.
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.

![Sub2008.test2008.lan.au Properties](image)

### 2.2 The iPrism Active Directory Account

The AD2008 user account that is created automatically by joining the iPrism to the Active Directory should 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`:

![Screenshot of the Account tab](image.png)
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:

![User Account Properties](image)
The minimum requirement is that the accounts are members of the *Domain Users* group, as shown in the following example:
3 iPrism Configuration

1. In the iPrism System Configuration Tool, select the System section, then the Networking tab. Ensure that the iPrism has a valid host name for the domain to which it will be joined.
2. Ensure that the DNS setting (**Name Server**) is set to a valid DNS that can resolve the fully qualified domain name of the AD server and the iPrism. In the following example, the AD server itself is used:
3. When joining the iPrism to the AD2008 domain, ensure that the **Machine Account** and **Domain Name** match your iPrism hostname (note that these are case-sensitive; verify that these are typed in the correct case):

![iPrism Authentication Configuration](image)

4. 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, iPrism may be unable to join the AD domain and clients may not be able to authenticate.

   **Important**: Windows networks generally use the Domain Controller as an NTP server. If this is the case, it is recommended that you set the iPrism to use the Domain Controller as its NTP server.

5. Click **Advanced**.

6. The IP address of your AD2008 server should be pre-populated in the IP Address field. If it is not, there is likely a configuration error in DNS. If you have multiple DNS servers serving out your AD domain, ensure that the IP address entered here is the AD server, and not that of a standalone DNS server.

7. Review the other query setting fields. **Important**: Do not change the Search User DN or Search User Password fields.

8. The following Encryption Types are available:
   - TLS/SSL
Note: Unless the AD Server has been set up with a server certificate, select **None**.

9. Click **Test** to test your settings.

![Advanced Settings for Server 2008](image)

10. If the Test is successful, click **OK** to return to the main window.

11. In the main window, click **Join**.

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

1. In the iPrism System Configuration tool, select the **System** section, then the **Preferences** tab.

2. Check **Use NTP** and enter the Domain Controller’s address in the **NTP Server** field.

3. Select the **Users** section, then the **Windows** tab.
4. Click **Advanced** and ensure that the correct IP address for the domain controller appears in the **IP Address** field:

![Active Directory Settings](image)

5. 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.)

6. 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

**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.
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\(^1\) in the **Proxy server** section of the **Local Area Network (LAN) Settings**:

\(^1\) 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:

1. Select **Tools → Internet Options → Security → Local Intranet → Sites → Advanced**.
2. Type the fully qualified domain name.
3. Click **Add**.
Internet Explorer must be configured for Integrated Authentication.

Verify this as follows:

1. Select **Tools → Internet Options → Security → Local Intranet → Custom Level**.
2. 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:

1. Type `about:config` in the address bar.
2. Search for the key `network.negotiate-auth.trusted-uris`.
3. 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

1. 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.

2. Add the domain name to the search suffixes.

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

4. 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.
5. 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

1. Open the Applications folder and browse to the Utilities folder.

2. From here, start up the Directory Utility application.
3. Click the + sign to add a directory. When that dialog opens, select *Active Directory* and you will see the following dialog:

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

5. 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.

1. Type your password.
2. 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:

1. Type `about:config` in the address bar.
2. Search for the key `network.negotiate-auth.trusted-uris`.
3. 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.