

# **R-1**

## **Deployment Platform**

# **PAM Configuration**

# **Guide**

**Software Version 5.0**

**For Linux and UNIX operating systems**

**May 9, 2011**

Copyright © 2011 RepliWeb® Inc., All Rights Reserved

The information in this manual has been compiled with care, but RepliWeb, Inc. makes no warranties as to its accuracy or completeness. The software described herein may be changed or enhanced from time to time. This information does not constitute a commitment or representation by RepliWeb and is subject to change without notice. The software described in this document is furnished under license and may be used and/or copied only in accordance with the terms of this license and the End User License Agreement.

No part of this manual may be reproduced or transmitted, in any form, by any means (electronic, photocopying, recording or otherwise) without the express written consent of RepliWeb, Inc.

Windows, Windows XP and Windows Vista are trademarks of Microsoft Corporation in the US and/or other countries. UNIX is a registered trademark of Bell Laboratories licensed to X/OPEN.

Any other product or company names referred to in this document may be the trademarks of their respective owners.

**Please direct correspondence or inquiries to:**

RepliWeb, Inc.  
6441 Lyons Road  
Coconut Creek, Florida 33073  
USA

Telephone: (954) 946-2274  
Fax: (954) 337-6424

Sales & General Information: [info@repliweb.com](mailto:info@repliweb.com)  
Documentation: [docs@repliweb.com](mailto:docs@repliweb.com)  
Website: <http://www.repliweb.com>

# Table of Contents

<b>1.</b>	<b>System Requirements .....</b>	<b>1</b>
	Windows .....	1
	Installing Identity Management for UNIX .....	1
	UNIX/Linux.....	2
<b>2.</b>	<b>Connecting a UNIX Machine to a Domain .....</b>	<b>3</b>
	Windows 2003 Server R2 Configuration .....	3
	UNIX/Linux Configuration: .....	3
	Editing Configuration Files: .....	3
	Joining a Domain: .....	6
<b>3.</b>	<b>Connecting to R-1 with a Domain User .....</b>	<b>7</b>
	<b>Appendix: Joining a Domain via SUSE GUI .....</b>	<b>10</b>

# 1. System Requirements

Make sure the participating machines meet these requirements before beginning.

**NOTE:** This chapter applies to machines without AD/LDAP for Linux or UNIX.

## Windows

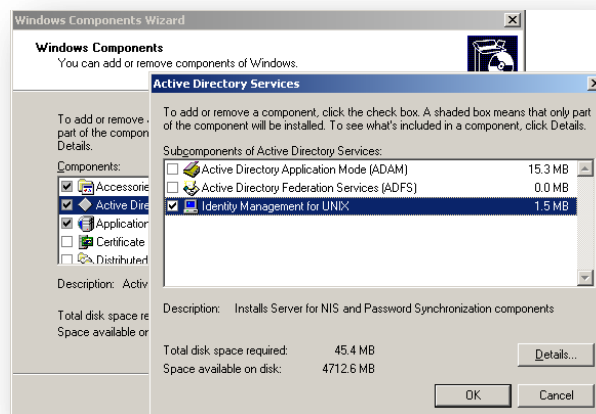
Before joining a UNIX machine to a domain, make sure **Windows Server 2003 R2** includes the **Identity Management for UNIX** component.

## Installing Identity Management for UNIX

**NOTE:** If your machine is not using an “R2” version server, you must download the **Microsoft Services for UNIX 3.5** component from Microsoft and either install it or upgrade you server to an “R2” version.

To install Identity Management for UNIX:

1. In **Control Panel**, open the **Add or Remove Programs** window and click the **Add/Remove Windows Components** button.
2. From the **Windows Components** wizard that appears, select the **Active Directory Services** checkbox and click the **Details** button.
3. From the **Active Directory Services** window that appears, select the **Identity Management for UNIX** checkbox.



4. Click **OK** to close the **Active Directory Services** window and then click **Next** to configure the new component.

**NOTE:** If needed, the configuration may prompt you to insert the **Windows Server 2003 R2** installation CD.

5. Click **Finish**.

## UNIX/Linux

Before you start the connection procedure, make sure **Samba** and **Winbind** daemons are installed and running at startup.

**NOTE:** The daemon installation process may differ depending on the UNIX/Linux flavor you are using.

## 2. Connecting a UNIX Machine to a Domain

### Windows 2003 Server R2 Configuration

To prepare Windows server:

1. After installing the **Identity Management for UNIX** component, a new scheme called **Unix Attributes** is added to the server. Right click a user, a dialog called “<User Name> Properties” appears.
2. Access the **UNIX Attributes** tab.
3. From the **Nis** domain, select the **domain Name**.

### UNIX/Linux Configuration:

Preparing the UNIX/Linux machine requires editing these files:

- /etc/hosts
- /etc/krb5.conf
- /etc/nsswitch.conf
- /etc/resolv.conf
- /etc/samba/smb.conf

Follow the steps below to edit these files on your UNIX/Linux machine. Alternatively, you can perform this procedure using SUSE GUI, as described in the [Appendix](#) section.

### Editing Configuration Files:

**NOTE:** In the examples below, Domain is “`unix.int`”, and Domain Controller FQDN is: “`dcunix.unit.int`”. Additionally, the UNIX Machine Host name is: “`suse01x3201`”.

To prepare UNIX/Linux server:

1. Go to `/etc/hosts` and either add or change to the following:

```
127.0.0.1      susi01x3201.unix.int susi01x3201 localhost
10.0.61.131   dcunix.unit.int dcunix
```

2. Go to `/etc/krb5.conf` and change to the following:

```
[libdefaults]
default_realm = UNIX.INT
clockskew = 300
```

```
[realms]
UNIX.INT = {
    kdc = dcunix.unix.int
    kdc = 10.0.61.131
    default_domain = unix.int
    admin_server = 10.0.61.131
}

[domain_realm]
.unix.int = UNIX.INT

[appdefaults]

pam = {
    ticket_lifetime = 1d
    renew_lifetime = 1d
    forwardable = true
    proxiable = false
    minimum_uid = 1
}
```

3. Go to `/etc/nsswitch.conf` and change to the following:

```
passwd: files winbind
shadow: files winbind
group: files winbind
protocols: files winbind
services: files winbind
netgroup: files winbind
automount: files winbind
```

4. Go to `/etc/resolve.conf` and change to the following:

```
search unix.int
nameserver 10.0.61.131
```

5. Go to `/etc/smb.conf` and change to the following:

```
# smb.conf is the main Samba configuration file. You find a
full commented
# version at
/usr/share/doc/packages/samba/examples/smb.conf.SUSE if the
# samba-doc package is installed.

[global]
    workgroup = UNIX
    printing = cups
    printcap name = cups
    printcap cache time = 750
    cups options = raw
    map to guest = Bad User
    include = /etc/samba/dhcup.conf
    logon path = \\%L\profiles\.msprofile
    logon home = \\%L\%U\.9xprofile
    logon drive = P:
```

```
usershare allow guests = No
idmap gid = 1000-30000
idmap uid = 1000-30000
realm = UNIX.INT
security = ADS
template homedir = /home/%D/%U
template shell = /bin/bash
winbind refresh tickets = yes
winbind enum users = yes
winbind use default domain = yes
winbind enum groups = yes
[homes]
comment = Home Directories
valid users = %S, %D%w%S
browseable = No
read only = No
inherit acls = Yes
[profiles]
comment = Network Profiles Service
path = %H
read only = No
store dos attributes = Yes
create mask = 0600
directory mask = 0700
[users]
comment = All users
path = /home
read only = No
inherit acls = Yes
veto files = /aquota.user/groups/shares/
[groups]
comment = All groups
path = /home/groups
read only = No
inherit acls = Yes
[printers]
comment = All Printers
path = /var/tmp
printable = Yes
create mask = 0600
browseable = No
[print$]
comment = Printer Drivers
path = /var/lib/samba/drivers
write list = @ntadmin root
force group = ntadmin
create mask = 0664
directory mask = 0775
```

## Joining a Domain:

To join the machine to a domain:

1. Restart the `smb` and `winbind` daemons by running these two commands:

- `/etc/init.d/smb restart`
- `/etc/winbind restart`

2. If these services restarted successfully, run the command:

```
net ads join -U administrator
```

3. When prompted, enter the password.

A message appears informing that the machine has joined the domain. If the join operation fails, try to either restart the services or restart both the machine and services, then rerun `net ads join -U administrator`.

4. To make sure that the machine has successfully joined the domain, complete one of the following steps:

- Go to the DC. In **Active directory Users and Computers**, search for the machine name.
- Run the `wbinfo -g` command. This command lists the groups in the domain.
- Run the `wbinfo -u` command. This command lists the users whose UNIX attributes you have defined.

**NOTE:** If running “`wbinfo -g`” or “`wbinfo -u`” fails with an error, restart the machine and then make sure the `Samba` and `Winbind` daemons are running.

## 3. Connecting to R-1 with a Domain User

To connect to R-1 with a domain user:

1. Install **R-1**.
2. Install **RTM** (Repliweb Topology Manager).
3. In UNIX, access the `/etc/pam.d` directory and create a file called "**repliweb**". Then, copy/paste the following PAM authentication rules into this file:

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is
run.

auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        sufficient    pam_ldap.so use_first_pass
auth        sufficient    pam_winbind.so use_first_pass
auth        required      pam_deny.so

account     required      pam_unix.so broken_shadow
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     [default=bad success=ok user_unknow=ignore]
pam_ldap.so
account     [default=bad success=ok user_unknow=ignore]
pam_winbind.so
account     required      pam_permit.so

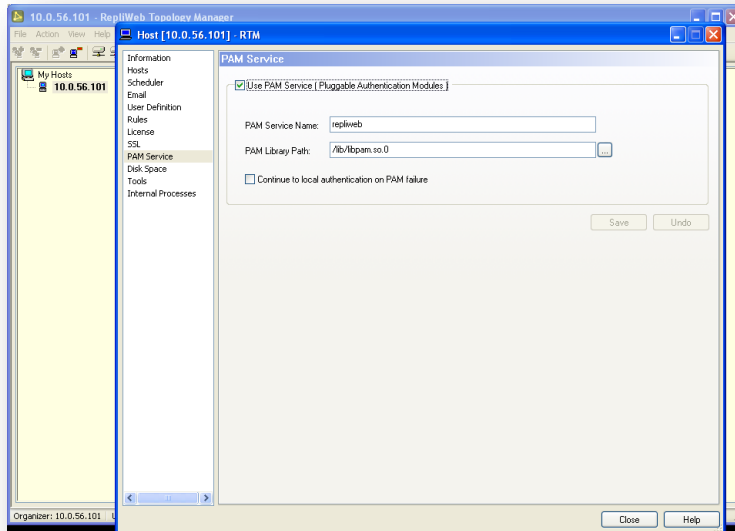
password    requisite     pam_cracklib.so try_first_pass
retry=3
password    sufficient    pam_unix.so md5 shadow nullok
try_first_pass use_authtok
password    sufficient    pam_ldap.so use_authtok
password    sufficient    pam_winbind.so use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so
service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_ldap.so
```

4. Connect with **RTM** to the machine.
5. In **RTM Manager**, add a new Host to the UNIX machine (i.e. the IP of the UNIX machine) by double clicking its IP.

The **RTM Manage** window appears for this UNIX machine.

6. Open the **PAM Service** tab.



- a. Select the **Use PAM Service** checkbox.
- b. In the **PAM Service Name** field, specify the file name you created in step 3 (`replweb`), without its path.

**NOTE:** PAM Service Name is case sensitive.

- c. In the **PAM Library Path** field, specify:

For 32-bit machines: `/lib/libpam.so.0`.

For 64-bit machines: `/lib64/libpam.so.0`

**IMPORTANT:** The `libpam` library can be stored in several possible locations (e.g., `/usr/lib/`) and may contain different suffixes. Please make sure the specified path and suffixes are accurate, otherwise PAM authentication will fail.

7. Select if to attempt local authentication in the event that PAM authentication fails.

**NOTE:** If the machine has a Centrify installation, make sure the **Continue to local authentication on PAM failure** checkbox is unselected. If PAM authentication is not successful, in the PAM configuration directory (default: `/etc/pam.d`), add the following lines inside the `/etc/pam.d/replweb` file mentioned above:

```

auth      sufficient      pam_centrifydc.so
auth      requisite      pam_centrifydc.so deny
account   sufficient      pam_centrifydc.so
account   requisite      pam_centrifydc.so deny
session   required          pam_centrifydc.so homedir
password  sufficient          pam_centrifydc.so try first pass
password  requisite          pam_centrifydc.so deny

```

8. Open **R-1 Console** and connect using a domain user's credentials.

**NOTE:** Provide the user's **Username** and **Password**, but leave the **Domain** field empty.

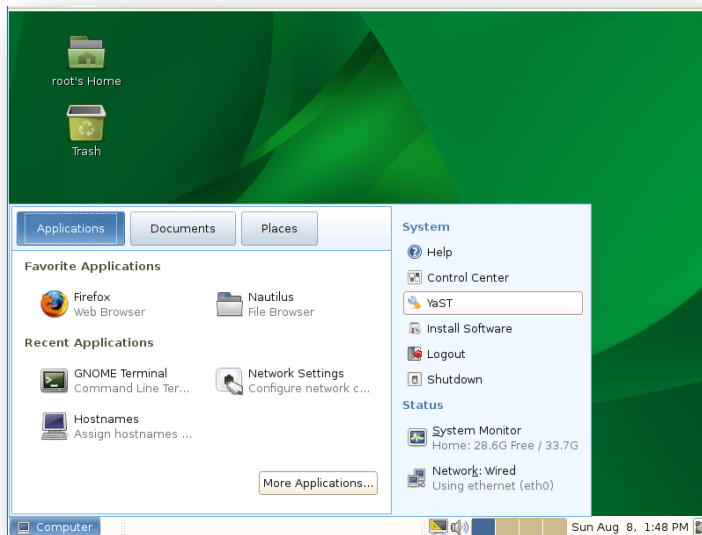
**NOTE:** When connecting to a UNIX machine, to avoid specifying a domain in the User Name field, add "**winbind use default domain = yes**" to the `/etc/samba/smb.conf` file's **[global]** section.

# Appendix: Joining a Domain via SUSE GUI

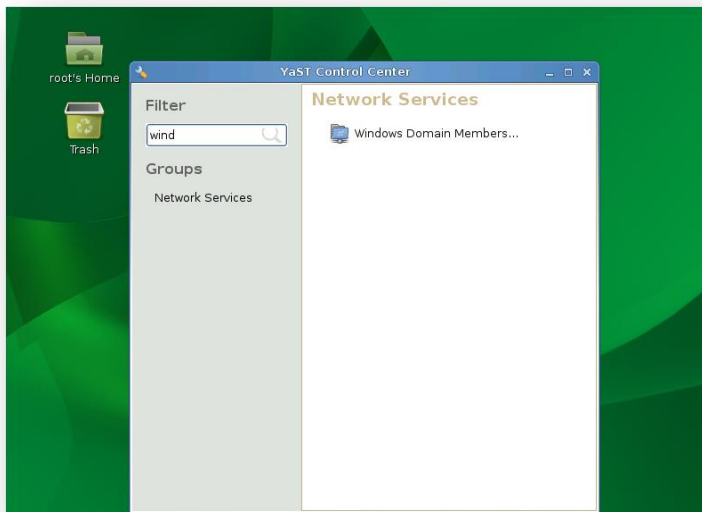
Use this procedure to join a UNIX/Linux machine to a Windows domain using SUSE GUI.

**To join a UNIX machine to a domain using SUSE GUI:**

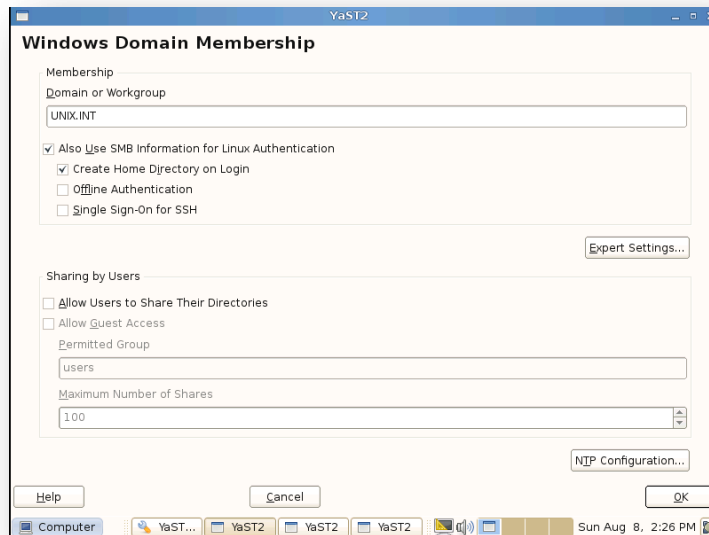
1. Log in to the machine as `root`.
2. Open **YaST** (Yet another Setup Tool).



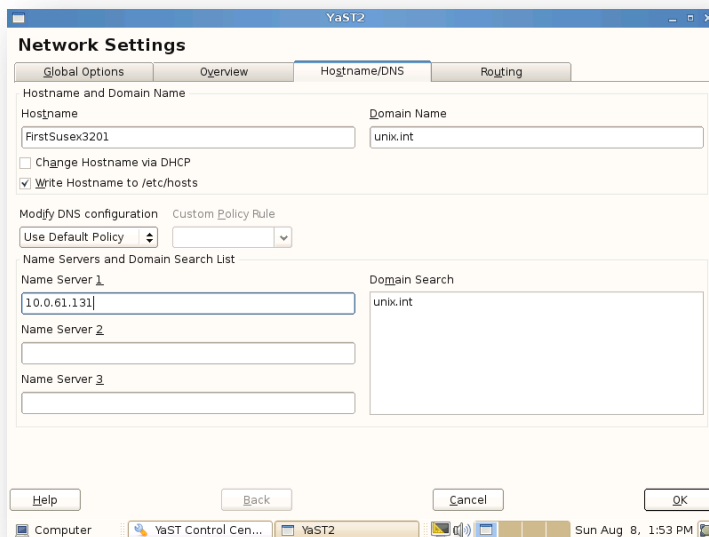
3. Search for the **Windows Domain Membership** network service:



#### 4. Open **Windows Domain Membership**.

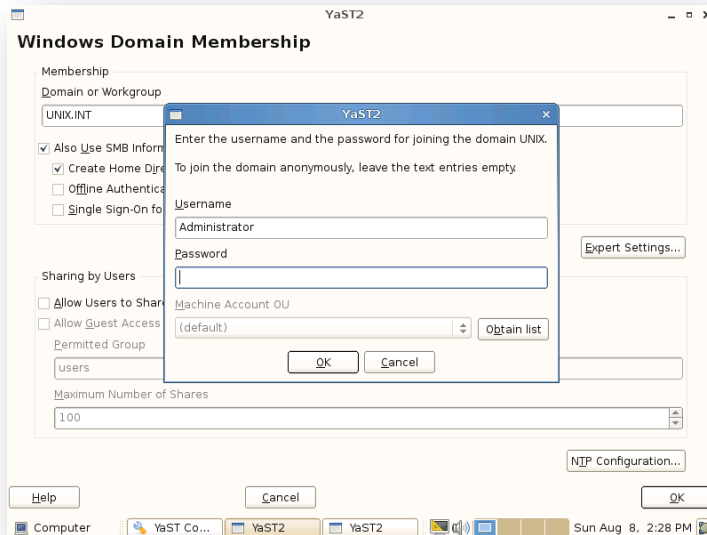


5. In the **Domain or Workgroup** field, enter the domain name. (In our example: “**unix.int**”).
6. Select the **Also Use SMB information for Linux Authentication** and **Create Home Directory on Login** checkboxes. (Do not click **OK** yet.)
7. Open **YaST** and search for **Network Settings**.



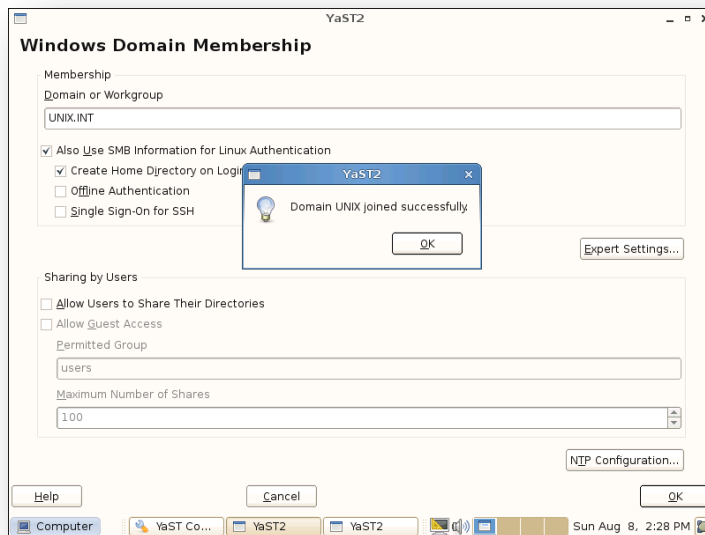
- a. Change the **Hostname**.
- b. Change the **Domain Name**.
- c. In the **Name Server 1** field, add the IP of the Domain Controller.
- d. Click **OK**.

- Return to the **Windows Domain Membership** window and click **OK**.
- When prompted, enter the Domain Controller's administrator password.



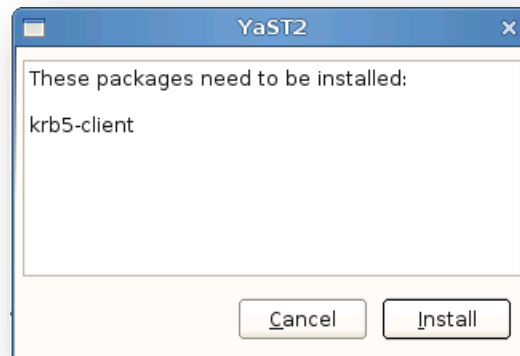
- Click **OK**.

If you properly configured the settings, the following message will appear: Domain <UNIX> joined successfully.



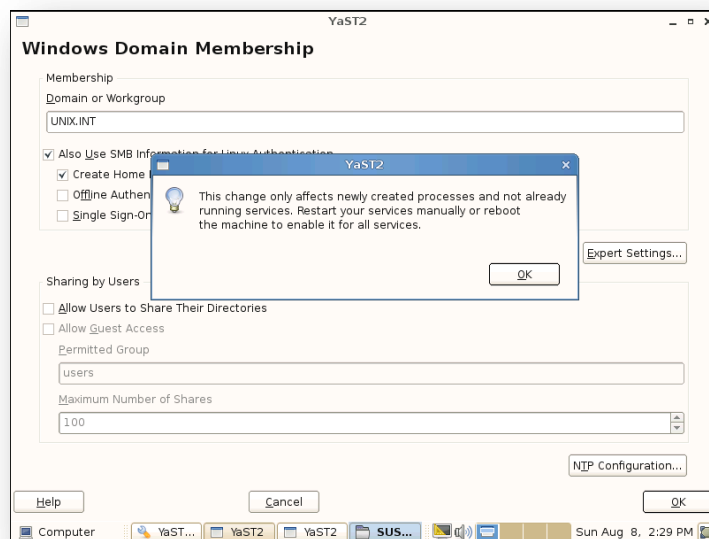
- Click **OK**.

12. When prompted, insert the SUSE installation CD.



13. Restart the `smb` and `winbind` services.

**NOTE:** These services must be started at startup.



14. Make sure the machine was successfully added to the domain:

- a. Open **Terminal**.
- b. Run the `wbinfo -g` command. This command lists the groups in the domain.
- c. Run the `wbinfo -u` command. This command lists the users whose UNIX attributes you defined.