

Windows Server Platforms - Joining Clients to win.mit.edu

Windows Server Platforms - Joining Clients to win.mit.edu

On this page:

- Warnings
- Quick Checklist
 - One-time considerations for new hosts and users:
 - General instructions:
- Moirra Requirements for the Machine and New Users
 - Moirra Record
 - DNS Propagation
- One-time Assignment of the Machine to a Container
- One-time Kerberos Password Update
- General Instructions
 - Reinstalling
 - Joining the Machine
 - Fast Boot
- First Maintenance of a Joined Client Machine
 - Clean Up Old Profiles on the Machine
 - Migrate the User's Local/Roaming Profile
- User First Impressions
- Related Links

Warnings

The container administrator and machine owner should be aware of certain naming considerations for your client machine. Further sources of information on this are the pages on [IP addresses](#), Host Names, and Domain Names and a form to [Request an IP address or Hostname](#).

The typical case of joining a machine to win.mit.edu, or WIN, involves the machine that resides in the MIT.EDU DNS domain. Special cases of machines that reside in a DNS subdomain at MIT, or reside in a DNS domain external to MIT.EDU, allow joining with a bit of manual work, but this document shows only the typical case.

Your machine with the official DNS name %COMPUTERNAME%.MIT.EDU when joining would routinely have the Active Directory, or AD, name of %COMPUTERNAME%. AD does not accept periods in computer names. Do not choose an AD name that is one of the aliases of the DNS name. For example, if your machine is TWISTY-NAME.MIT.EDU but has TWIST.MIT.EDU as an alias, the AD name must be TWISTY-NAME, not TWIST. Failure to adhere to this convention may result in unpredictable or undesirable behavior. Also, do not use an AD name longer than eleven (11) characters. AD may not use the extra characters of machines with longer names, so two machines with the same first 11 characters would conflict with each other.

Aliases can be as long as you like. This means that instead of having a machine whose official name is TEDIOUSLY-LENGTHY-APPELLATION with alias TLA, you should register the machine's official name to be TLA with alias TEDIOUSLY-LENGTHY-APPELLATION. If you already have the machine registered with the longer name, you should request from Moirra that the alias and the official names be switched, so the shorter name becomes the official name, and the longer becomes the alias. You can do this by sending an email to net-help@mit.edu requesting the proposed name changes and including the IP address plus old and new names.

Quick Checklist

One-time considerations for new hosts and users:

- Is there a Moirra record for the machine which has propagated to the MITnet DNS?
- Has the machine been assigned to a container?
- Is your Kerberos password up-to-date?

General instructions:

- Before reinstalling or rejoining a machine, the old machine account must be deleted from the AD, but no change to the Moirra records is

needed. To delete the existing machine account in the AD only, the machine owner or the container admin should use the web form located on the [Domain Machine Management page](#).

- Remove existing (non-WIN) MIT Kerberos software and reboot
- Verify correct IP and DNS settings, join machine to domain and reboot

If no packages are downloaded, reboot a second time due to the XP fast boot default.

Moirra Requirements for the Machine and New Users



Note: This step is **not** required for reinstalling.

Moirra Record

Every machine in WIN must have a host record in the Moirra database, which propagates out to a DNS record on the MITnet DNS servers. You can check if your hostname or IP is already registered using the stella command on a Unix Athena machine by typing `stella hostname` or `stella IP` to query the database. If you require a new record, [request an IP address](#).

DNS Propagation

In the example below, the record has a Status of Reserved (0). Your host record should have a Status of Active (1), or no DNS record will be created.

```
athena% stella foo
Machine: FOO.MIT.EDU
Address: unassigned Network: NONE
Owner: NONE Use data: 08-dec-1993 14:56:23
Status: Reserved (0) Changed: 23-feb-2001 18:07:22
Vendor: Location:
Model: Contact:
OS: Billing Contact:
Opt: 0 Account Number:
Adm cmt:
Op cmt:
```

Also, if you request that a new record be created, it may take another business day for the database records to be propagated to the DNS records, so you should verify that DNS record. You can ping the hostname to see if it resolves to an IP, use `nslookup` or the `hostinfo` command: `hostinfo foo` or `nslookup foo`.

One-time Assignment of the Machine to a Container

In order for a machine to get the group policies and MSI packages it requires to function properly in the domain, it must be assigned, in Moirra, to a container that is within the "Machines" container in AD. If there is no assignment, the machine will appear in the "Orphans/Machines" container and not get the group policy objects it needs.

The typical machine to be joining the WIN Domain resides in the mit.edu DNS domain. A separate document will treat special cases of machines that reside either in a DNS subdomain at MIT, or reside in a DNS domain external to mit.edu.

You can use the stella command to assign the container; `stella hostname -lcn` lists the container if one has been assigned, the `-dcn` option removes an existing machine-to-container assignment, and `-acn` adds one. Perhaps this query is a good candidate for a future web application.

To check if a host already has been assigned to a container use the `-lcn` option:

```
athena% stella foo -lcn
Machine: Container: Machines/pismere-laptops
```

If the machine has not been assigned to a container, you will not get any output from the previous command. To assign the machine to a container use the `-acn` option:

```
athena% stella foo -acn Machines/pismere-laptops
```

If the machine already has been assigned to a container, but you wish to move it to another one, you must first delete the old container assignment using the `-dcn` option, then assign it to the new container with `-acn`:

```
athena% stella foo -dcn Machines/pismere-laptops
athena% stella foo -acn Machines/pismere-dev
```

It should now show up as belonging to the new container:

```
athena% stella foo -lcn
Machine: FOO.MIT.EDU Container: Machines/pismere-dev
```

One-time Kerberos Password Update

If the user's password has not been changed since July of 2000, an error will occur when logging into a machine in the win.mit.edu domain. To solve this problem, have the user change their Athena, aka Kerberos, password using Leash32 on any Windows workstation, or Leash on any Macintosh that has the MIT Kerberos libraries installed on it. The user alternatively may use the `passwd` command on a Unix Athena workstation.

The password change is required to resolve a configuration conflict between the MIT Kerberos server and the Microsoft implementation of Kerberos version 5. Once the Kerberos password changes in the Athena realm, the user should be able to log on to any WIN machine.

General Instructions

Reinstalling

Before reinstalling or rejoining a machine, the old machine account must be deleted from the AD, but no change to the Moira records is needed. To delete the existing machine account in the AD only, the machine owner or the container admin should use the [web form](#) located on the Domain Machine Management page.

Joining the Machine

Be sure the machine is properly patched before connecting to the network. Verify the proper IP and DNS information. The machine should use the following three MIT DNS servers: 18.72.0.3, 18.70.0.160 and 18.71.0.151.

Remove existing MIT Kerberos and packages that did not come from a WIN distribution. We have seen compatibility issues in the past where users could not logon using other Kerberos distributions. The existing packages should be removed via the Add-Remove Programs control panel, then the machine should be rebooted before joining.

Join the machine to the domain using the System control panel. Select the network identification tab and click on properties. Verify that the machine name is the same as the name used in its Moira record. If it is not, you will need to change it to that name and reboot. Otherwise, change the domain name to win.mit.edu and click OK. You will then be prompted for a username and password; use the win/Kerberos account credentials and click O*K*. If successful, you will get a message saying "Welcome to the win.mit.edu domain." After answering this prompt you will be asked to confirm the choice to reboot.

In steps, here is the recipe:

1. [Add the machine to your container.](#)
2. Log on to the machine as local administrator.
3. Right click the **My Computer** icon (or the computer name might be displayed under the icon).
4. Select **Properties**.
5. Click the **Network Identification** tab.
6. Click the **Properties** button.
7. Select the **Member of Domain** radio button.
8. Type in: WIN.MIT.EDU (in all capitals).
Result: You will get a screen welcoming you to the domain.
9. Reboot the machine for the changes to take effect.

Fast Boot

Windows machines, by default, bring up the logon "Press Ctrl-Alt-Delete" dialog box before Group Policy settings have been applied. These machines perform a background refresh of Group Policy at boot time. However, certain types of policy, like Software Installation and Folder Redirection, cannot take place during a background refresh. Instead, these machines will take new MSI software and folder redirection at some subsequent boot. You may need to reboot a machine before you can guarantee that the machine has fully taken Group Policy.

The WIN domain has the following Group Policy setting enabled: "Computer Configuration/Administrative Templates/Windows Components/System/Logon/Always wait for the network at computer startup and logon." However, there is a "Catch 22" situation when joining a new machine because group policy must be downloaded to the machine for the behavior to change. For this reason, it is sometimes necessary to reboot a machine again before it can initiate the install of the MSIs that have been assigned via group policy.

Once MSIs have been installed, it is good practice to check the Application log for any failed MSI installations, and verify functionality by logging on to the machine with a Kerberos username and password.

Problems with machine joins should be reported to network-win@mit.edu -->

First Maintenance of a Joined Client Machine

Clean Up Old Profiles on the Machine

When a client machine has been joined to the domain, any existing profile, even the default user, becomes obsolete. The local administrator may choose to dispose of these in a number of ways, but it would be decent to allow the user to move and delete them as follows:

1. Log on as local administrator.
2. Locate the user's profile either on the server or the local machine.
3. Set full control permissions to the user's WIN account.
4. Log back out.

Migrate the User's Local/Roaming Profile

1. Have the user log on using his/her Kerberos principal and (new) password.
2. Map back the user's previously existing network drives.
3. Locate the user's profile (either on a server or the local machine) and copy all the folders to:
`C:\Documents and Settings\ username`



Note: The user's desktop icons should reappear, but the wallpaper might be lost. There may be some file locks on files contained in the profile (Cookies, for example); generally, these locked files are `index.dat` files.

4. Select all files except those named `index.dat` and copy them to the appropriate folder. A reboot of the machine should release locks on these files and save some time.
5. Launch Microsoft Office applications (Word and Excel) once, so the user settings will be gathered and stored in the Roaming Profile.
6. Launch Outlook, Global Protect VPN, Word, SAP, etc., making sure all applications work.
7. Bring back bookmarks for your browser. (If bookmarks are stored on a server, reset the profile to point to the server).
8. For IE, if the user saved a Favorites file, import it back in to the user's IE favorites list.
9. Log out and notice that the roaming profile will be saved. Next time the user logs on, the roaming profile should be migrated.

User First Impressions

Perhaps the user first notices the new mapped drive `H:`. `H:` is the user's home directory by default on DFS. Looking carefully between logins, the user can see the roaming profile, caches, settings and such files saved to `H:`. The user can now utilize this `H:` drive as remote storage for backups, data files or even programs.

Related Links

- [The win.mit.edu Domain](#)
- [Windows Server Platforms](#)
- [WIN.MIT.EDU Landing Page](#)
- [Windows Server Software Landing Page](#)