

Use only letters (A-Z) and numbers (0-9) in your computer names. Hyphens, underscores, and other characters may cause problems with your DNS Servers.

Do not start your computer name with a numerical character. Not all DNS Servers expect to see a DNS name that starts with a number, and may interpret it incorrectly.

Keep your computer names under 15 characters in length. Avoid using terms and words that are difficult to spell, or sounds like other words. (i.e. Check and Czech).

Avoid using usernames as the computer name. This creates an Administrative nightmare when you replace a users PC, or if you give the PC to a different user. Try using a simpler and impartial naming scheme based on location and department.

Use colors for server computer names. Using the seven basic colors, red, orange, yellow, green, blue, indigo and violet, should cover most server environments. Large data center would need to use a slightly different naming convention do to the large number of servers.

Place a small label or tag on the front of every server to identify its computer name. On workstations, place the stickers on the sides of the computer case and out of view from the users to prevent them from peeling them off.

Common coding abbreviations

SV Servers

IIS Web Servers

WS Workstations

MSX Mail Servers

PR Printers

SQL SQL Servers

TS Terminal Servers

SMS SMS Servers

DC Domain Controllers

APP Application Servers

Servers: A server named RED at the Headquarters in Worcester that is also the Domain Controller would look like "WORSVDCRED"
LOCATION + TYPE + NAME

Workstations: A workstation numbered 01 located at the Headquarters in Worcester's Human Resources department would look like "WORWS01HR"
LOCATION + TYPE + NUMBER + DEPARTMENT

The purpose of defining levels of access for employees is to achieve a streamlined protocol for adding and deleting employees, contractors, and others needing access to the network.

Once the levels are developed, Cinch IT will know exactly which folders and applications each user needs to be configured for.

Defining levels makes termination a much safer and streamlined process that leaves no room for error in the event of not removing an employee from an overlooked access point.

The four steps below explain the procedure:

1. **List all employees**
2. **List all departments**
3. **Group employees into each department**
4. **Define levels of access to apply to each department as well as list each application each department should be enabled for.**

Level 1 is the highest level of access with the exception of Administrator; this should only be granted to technical employees.

Level 2 and beyond will be defined by each company based on specific needs.

Cinch IT can assist in developing these protocols or each corporation can define them and Cinch IT will help deploy efficiently.