[Server setup guide and Documentation]

[This document is intended to define the setup and best practices for servers in the domain]

[Evan Schober CIS223]

Contents

[General Overview 1](#_Toc480436084)

[Physical security 1](#_Toc480436085)

[Updates and Anti-virus 1](#_Toc480436086)

[Naming Conventions 1](#_Toc480436087)

[Device Type 2](#_Toc480436088)

[Geographic Location 2](#_Toc480436089)

[Building/Site location 2](#_Toc480436090)

[Department 2](#_Toc480436091)

[Placeholder Characters 3](#_Toc480436092)

[Device Number 3](#_Toc480436093)

[Setup Instructions 3](#_Toc480436094)

[Server Installation 3](#_Toc480436095)

[Roles 3](#_Toc480436096)

[Sever Objects 3](#_Toc480436097)

[Domain Controllers 3](#_Toc480436098)

[Sites 4](#_Toc480436099)

[Organizational Units (OUs) 4](#_Toc480436100)

[User Accounts 4](#_Toc480436101)

[Account Creation 4](#_Toc480436102)

[Password Creation & Resets 4](#_Toc480436103)

[Account Retention 4](#_Toc480436104)

[Temporary Accounts 5](#_Toc480436105)

[File Sharing 5](#_Toc480436106)

[Departmental Shares 5](#_Toc480436107)

[User Access 5](#_Toc480436108)

[Group Policy 5](#_Toc480436109)

[Security Options 5](#_Toc480436110)

[Password Policy 5](#_Toc480436111)

[Account Lockout Policy 5](#_Toc480436112)

[Audit Policy 5](#_Toc480436113)

[User Rights 6](#_Toc480436114)

[Networking 6](#_Toc480436115)

[DHCP 6](#_Toc480436116)

[IPV4 6](#_Toc480436117)

[IPV6 6](#_Toc480436118)

# General Overview

## Physical security

Servers should be contained within a dedicated controlled access server room. Dedicated fire suppression and redundant power should be a consideration of the construction of this room. Dedicated room cooling and/or air filtration & circulation is a minimum requirement for all rack-mount hardware.

A minimum of three physical copies of this server documentation should be kept up to date at all times. One copy is to be kept near the physical server hardware for easy reference when direct access to the server is necessary. The second copy should be kept in the system administrator’s office. The third copy is to be kept secured such that it is protected from natural hazards such as fires, flooding, etc.

This document is to be updated in a timely fashion following changes.

## Updates and Anti-virus

The default anti-virus settings are configured.

Server updates are to be administered within a virtual environment and tested to ensure compatibility. Once the safety of the upgrade has been determined an image of the current machine state will be made prior to administering the upgrade to the host server.

This document is to be updated following any changes to the server. As such the system history contained here can be used to determine the cause in the event of a system failure.

## 

## Naming Conventions

All devices on the network will be given a name following the standard shown here. It consists of the following parts. Details for the use and assignment of each part are listed below.

1. Single character “Device Type Identifier”
2. Three character location code
3. Three-digit building/site number
4. Three-digit department number
5. Two character demarcation/placeholder
6. Three-digit device number



The following sections contain tables listing the available device types and location identifiers as well the ID numbers for buildings, departments, and devices.

### Device Type

Devices will be identified with a single character as listed in the table below:

|  |  |
| --- | --- |
| Device type | Character Identifier |
| Server | S |
| Workstation (Desktop) | W |
| Laptop | L |
| Virtual (VDI) | V |
| Tablet | T |
| Printer | P |
| Phone (Mobile) | M |

### Geographic Location

Device location will be identified with a 3 character code. As often as possible this should be a selection of consecutive or semi-consecutive characters within the name of the largest neighboring city.

E.g. **K**alama**ZO**o = KZO

|  |  |
| --- | --- |
| Device Location | Identifier |
| Kalamazoo | KZO |

### Building/Site location

Facilities located within a given geo-political area (listed above) will be assigned a three digit numerical identifier. These numbers will be assigned sequentially as new facilities are brought on board. A complete list of these ID numbers will be kept for each geographic location.

|  |  |
| --- | --- |
| Building Name | ID Number |
| Headquarters | 001 |

### Department

Departments will receive a randomly assigned three-digit identifier.

|  |  |
| --- | --- |
| Department | ID Number |
| Administration  (C-levels) | 233 |
| Human Resources | 727 |
| Accounting | 338 |
| IT | 904 |
| Food Services | 360 |
| Maintenance | 040 |
| Marketing | 010 |
| Purchasing | 976 |

### Placeholder Characters

This two character space is designed to allow for future expansion of the naming standard without adding additional complexity. Until such a time as this space becomes necessary these two characters should always be “XX”

### Device Number

Device numbers will be assigned sequentially for each device type in each area as defined by location, building and department.

# Setup Instructions

## Server Installation

To ensure system stability and allow for future growth all server hardware must meet or exceed the recommended requirements for the operating system being installed. Hardware not meeting the requirements for OS upgrade must be upgraded, replaced, or left with the compatible version of the operating system.

Initial installation is configured as a role based server running Windows 2012 Datacenter. It is configured with the roles listed below. It can be contacted via MSTSC.exe at 10.0.2.15. The server’s name is SKZO001904XX001.home.SchobCorp.net/SysAdmin and the password is EyE8SumPi

## Roles

As additional servers being to take on different aspects of the network, different roles will need to be configured. However, for servers intended as domain controllers, initial setup should include the following roles:

* Active Directory Domain Service
* DHCP
* DNS
* Web Server (IIS)

All roles are configured with default settings.

Only after a static IP has been configured and the roles have been installed may the server be promoted to a domain controller.

# Sever Objects

## Domain Controllers

Domain controllers will be configured

## Sites

## Organizational Units (OUs)

Organizational units will be configured for each department the name of which

OUs

# User Accounts

## Account Creation

User accounts are to be created only after an offer of employment has been extended to a prospective employee. Accounts are disabled by default until users have completed the Network Access Agreement Form (NAAF). This form is a contract requiring users to abide by the rules of the network as well as provide a selection of security questions and ensure that customer support and IT security have relevant contact information for each employee.

User accounts will be created within their department specific parent and child OUs.

Accounts awaiting completion of the user’s NAAF will be labeled with the description \*Awaiting NAAF\*

## Password Creation & Resets

Account passwords are **not** to be created upon account creation.

Passwords will be made available only after users have submitted their NAAF. At which point users’ accounts will be enabled and a temporary password will be given to them at the time of orientation.

Passwords that have not expired may be reset with the password reset tool available on the SchobCorp intranet home page.

Acquiring or resetting a password outside orientation or after the password has expired must be completed via a phone call to IT Customer Support.

## Account Retention

Prospective employees who reject an offer of employment will have their accounts deleted immediately.

Following departure from SchobCorp user accounts will be immediately disabled but be retained for a maximum of 30 days. Account descriptions will be modified to reflect the date on which the account will be deleted. In circumstances where an account must be retained for legacy or legal reasons disabled accounts may be retained indefinitely.

Accounts being held beyond the default retention policy must be labeled to reflect this.

## Temporary Accounts

Temporary accounts for contractors, interns, students, etc. will follow the same creation, deletion and retention rules set for standard employees. However, their accounts will be configured via active directory to automatically expire at the end of their term with SchobCorp.

Temporary accounts will be labeled with their start and end dates.

# File Sharing

## Departmental Shares

All departments will be given shared folders within the universal network shared drive. Individual folder access will be controlled with departmental group policy.

Departmental users will be given all permissions to files and folders within their Department’s shared folder but will be denied full control.

Department managers will have full control of all files and folders within their departmental shares.

## User Access

# Group Policy

## Security Options

Accounts: Administrator and Guest accounts are to be disabled.  
Audit: Shut the system down immediately if unable to log security audits.  
Interactive Login: Display user information when the session is locked.  
Interactive Login: Prompt user to change password before expiration.

## Password Policy

User passwords must be at least 8 characters long.   
Passwords must meet the complexity requirements.   
Passwords have no minimum age.  
Passwords expire 6 months after they are set.  
The last 10 passwords will be remembered.

## Account Lockout Policy

Accounts will be locked out after 5 invalid login attempts within a 10 minute period.   
Accounts will automatically unlock 15 minutes after they become locked.

## Audit Policy

## User Rights

# Networking

## DHCP

### IPV4

### IPV6