LUPIN

STANDARD OPERATING PROCEDURE

Corporate IT

No.: ITP-018-03	ACTIVE DIRECTORY AND LAN SECURITY SERVICES	Effective Date: 11/01/2017
Supersedes: ITP-018-02		Review Period: 3 Years

1.0 PURPOSE:

This Standard Operating Procedure (SOP) is designed to improve the centralized manageability, security and delegation of administrative control over the Lupin's network comprised of windows clients, windows servers and windows compatible application and devices.

2.0 SCOPE:

Applicable to all Microsoft Windows servers, desktops, Laptops and other network devices compatible to Microsoft Windows operating system within the network.

3.0 RESPONSIBILITY:

Server Administrator and HOT IT Infrastructure shall be responsible for execution of this SOP. HOT IT Infrastructure shall be responsible for compliance of this SOP at all the Lupin sites.

4.0 DEFINITION:

Active Directory - Active Directory is Microsoft's trademarked directory service, an integral part of the Windows 2000/2003/2008 or higher version architecture. Like other directory services, such as Novell Directory Services (NDS), Active Directory is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories.

	PREPARED BY	REVIEWED BY	APPROVED BY
SIGN & DATE	07/12/2016	7/12/2016	07/12/2016
NAME	Rajesh Bind	Jay Baksh	Amit Bhaskar
DESIGNATION	Sr. Executive I.T.	SR. GM-IT	GM – CQA

No.: ITP-018-03	ACTIVE DIRECTORY AND LAN SECURITY SERVICES

5.0 PROCEDURE:

5.1 The Lupin shall use a Microsoft Windows 2008 Active Directory Service or higher version. Active directory services shall be installed according to Annexure 1.

5.2 Server Administrator shall ensure proper naming convention is used while adding new domain or child domain in the forest.

5.3 Ensure that DNS shall be installed and configured as core component of Active directory.

5.4 The date and time on all the computers (Servers, Desktop and Laptop) shall be synchronized with Domain Controller. Nobody shall be able to change them on his/her computer.

5.5 All computers and mobile devices running a Microsoft Windows operating system or an operating system that interoperates with Windows Domain and that are connecting to Lupin's Network are required to join the "Lupin" Windows Domain at the time of installation.

5.6 Server administrator shall create one Desktop admin account and delegate rights of desktop local administrator to this account for day to day routine administrative activities.

5.7 Server administrator shall create service accounts and assign proper permissions according to the roles.

5.8 For new user IT department shall create domain user based on information received from HR/Respective department.

5.9 IT department shall give file and print sharing access at the time of user creation or as per the proper request from the respective department head.

5.10 IT department shall immediately disable account of left employee after receiving relieving form from HR department.

5.11 Server administrator shall create OU structure on the basis of physical location.

	PREPARED BY	REVIEWED BY	APPROVED BY
SIGN & DATE	07/12/2016	7/12/2016	07/12/2016

5.12 Account Password Policy shall be configured as follows.

- Enforce password history - 5 passwords remembered
- Maximum password age - 42 days
- Minimum password age - 1 day
- Minimum password length - 8 characters
- Password must meet complexity requirements – Enabled
- Store passwords using reversible encryption – Disabled

5.13 Account Lockout Policy shall be configured as follows

- Account lockout duration - 10 minutes
- Account lockout threshold - 3 invalid logon attempts
- Reset account lockout counter after –10 minutes

5.14 Account Kerberos Policy shall be configured as follows

- Enforce user logon restrictions - Enabled
- Maximum lifetime for service ticket - 600 minutes
- Maximum lifetime for user ticket - 10 hours
- Maximum lifetime for user ticket renewal - 7 days
- Maximum tolerance for computer clock synchronization - 5 minutes

5.15 Account System Policy shall be configured as follows

- Turn Off Autoplay – Enabled for All Drives

5.16 Event and Audit Policy shall be configured as follows

- Maximum application log size - 16384 KB
- Maximum security log size - 20480 KB
- Maximum system log size - 16384 KB
- Retention method for application log - Overwrite
- Retention method for security log - Overwrite
- Retention method for system log - Overwrite
- Audit account logon events - Success, Failure
- Audit account management - Success, Failure
- Audit logon events - Success, Failure

- Audit object access - Success, Failure
- Audit policy change - Success, Failure
- Audit system events - Success, Failure

5.17 All PC's , Desktops and Laptops shall be running with Services as per agreed configuration attached in Annexure 2 for Windows XP as well as Windows 7.

5.18 Time format shall be HH:mm:ss. Date format shall be dd/MM/yy. Group policy setting shall be done according to Annexure 3 for Date & Time settings.

6.0 ABBREVIATIONS:

ITP	:	Information Technology Procedure
IT	:	Information Technology
DNS	:	Domain Name Service
OU	:	Organizational Unit
ADS	:	Active Directory Services
HOT	:	Head of Technology
SOP	:	Standard Operating Procedure
HR	:	Human Resources

7.0 REFERENCES:

NA

	PREPARED BY	REVIEWED BY	APPROVED BY
SIGN & DATE	07/12/2016	7/12/2016	07/12/2016

No.: ITP-018-03	ACTIVE DIRECTORY AND LAN SECURITY SERVICES

8.0 ANNEXURES:

Annexure 1 : Installation of Active Directory Services and LAN Security Services.
Annexure 2 : Window's XP and Window 7 Services running on local desktop laptop
Annexure 3 : Group Policy setting for date & time

REVISION HISTORY

Version No.	Effective Date	Details of Review / Revision
00	10/08/2009	New Document.
01	12/08/2011	Revised Document.
02	15/01/2014	Revised Document Following changes are done : • A new Annexure 3 incorporated for Group Policy settings for Date & Time. • Section 5.1 modified for the version of Windows
03	11/01/2017	Revised Document • Section 5.3 to 5.19 is renumbered to 5.2 to 5.18 respectively. • Section 6.0 is updated for abbreviations.

	PREPARED BY	REVIEWED BY	APPROVED BY
SIGN & DATE	07/12/2016	7/12/2016	07/12/2016

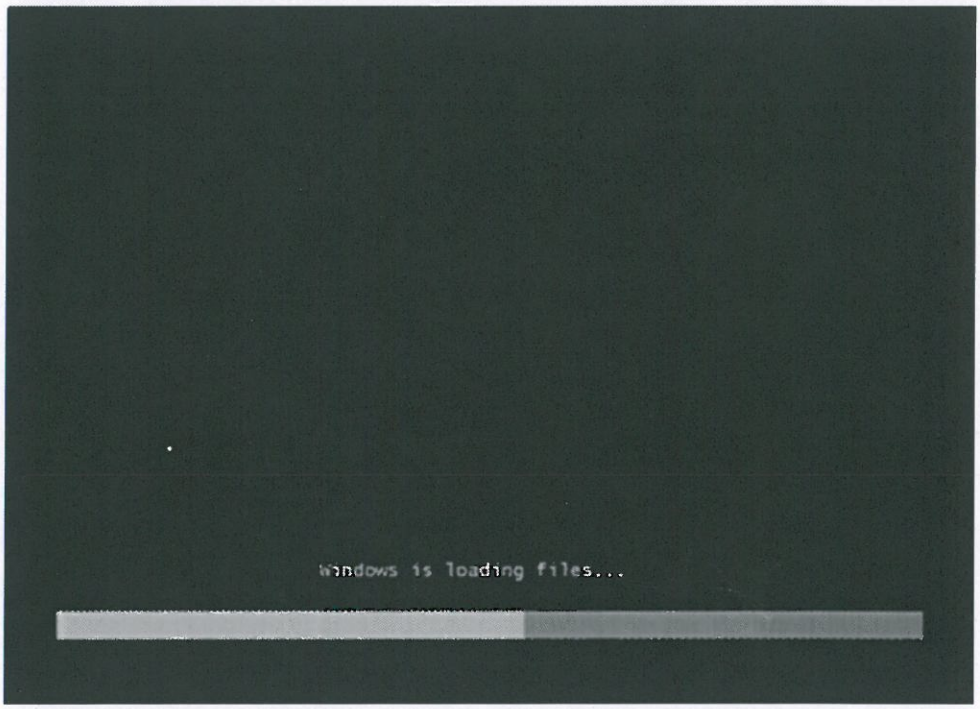
Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Follow this procedure to install Windows Server 2008 Standard 64 Bit R2

Step1: Insert the appropriate Windows Server 2008 Standard 64 Bit R2 installation media into your DVD drive. Page (1/1).

Step 2: Reboot the computer. Page (1/1).

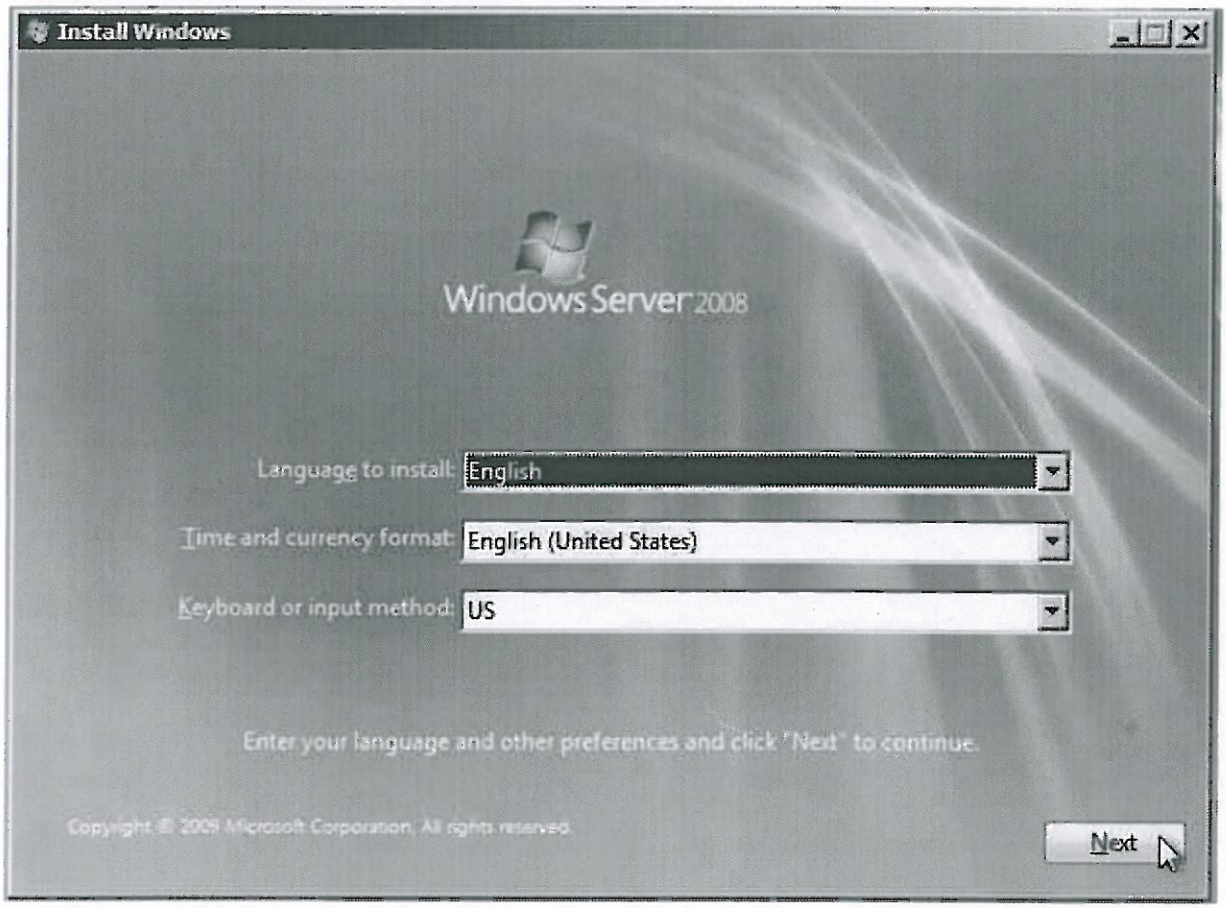


07/12/2016 7/12/2016 07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 3: When prompted for an installation language and other regional options, make your selection and press Next. Page (1/1).

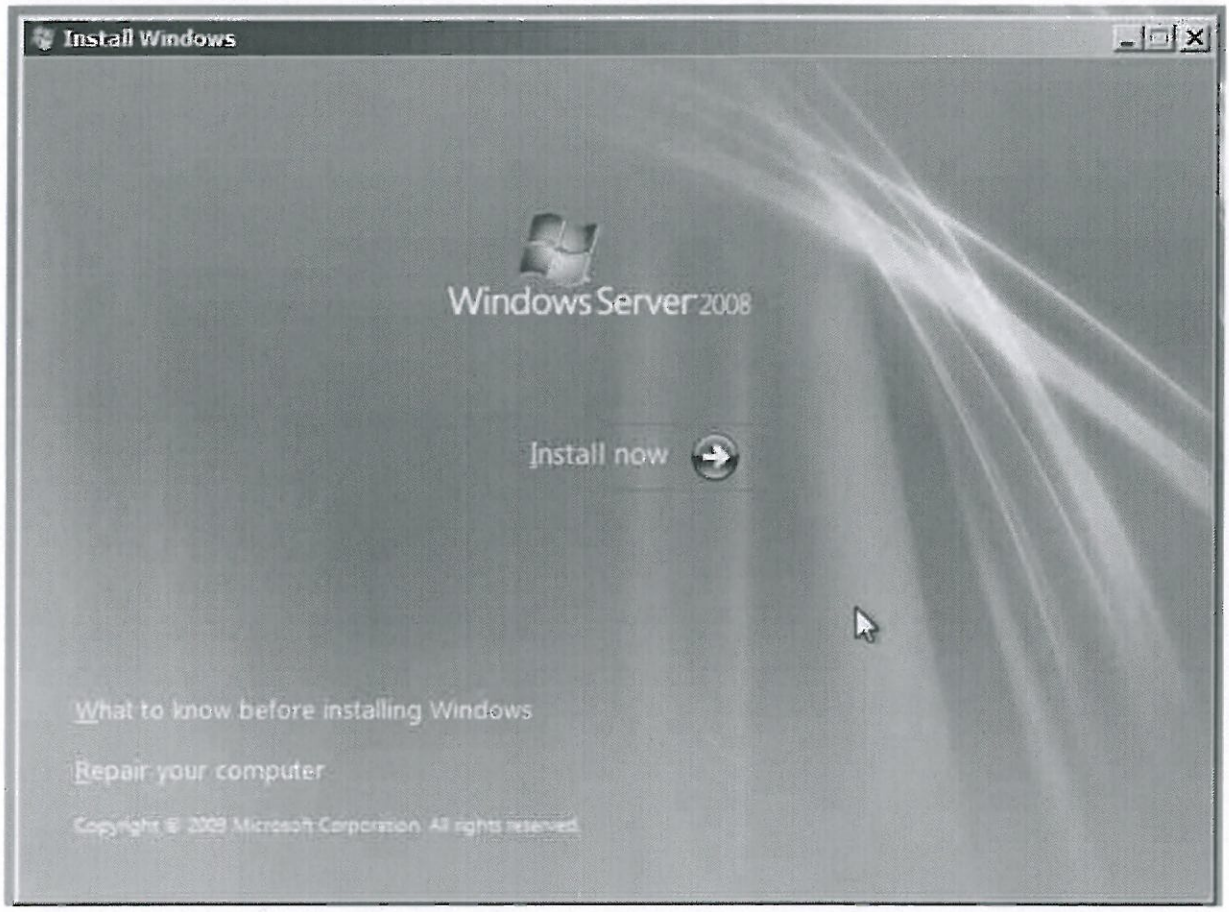


07/12/2016 7/12/2016 07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 4: Next, press Install Now to begin the installation process. Page (1/1).



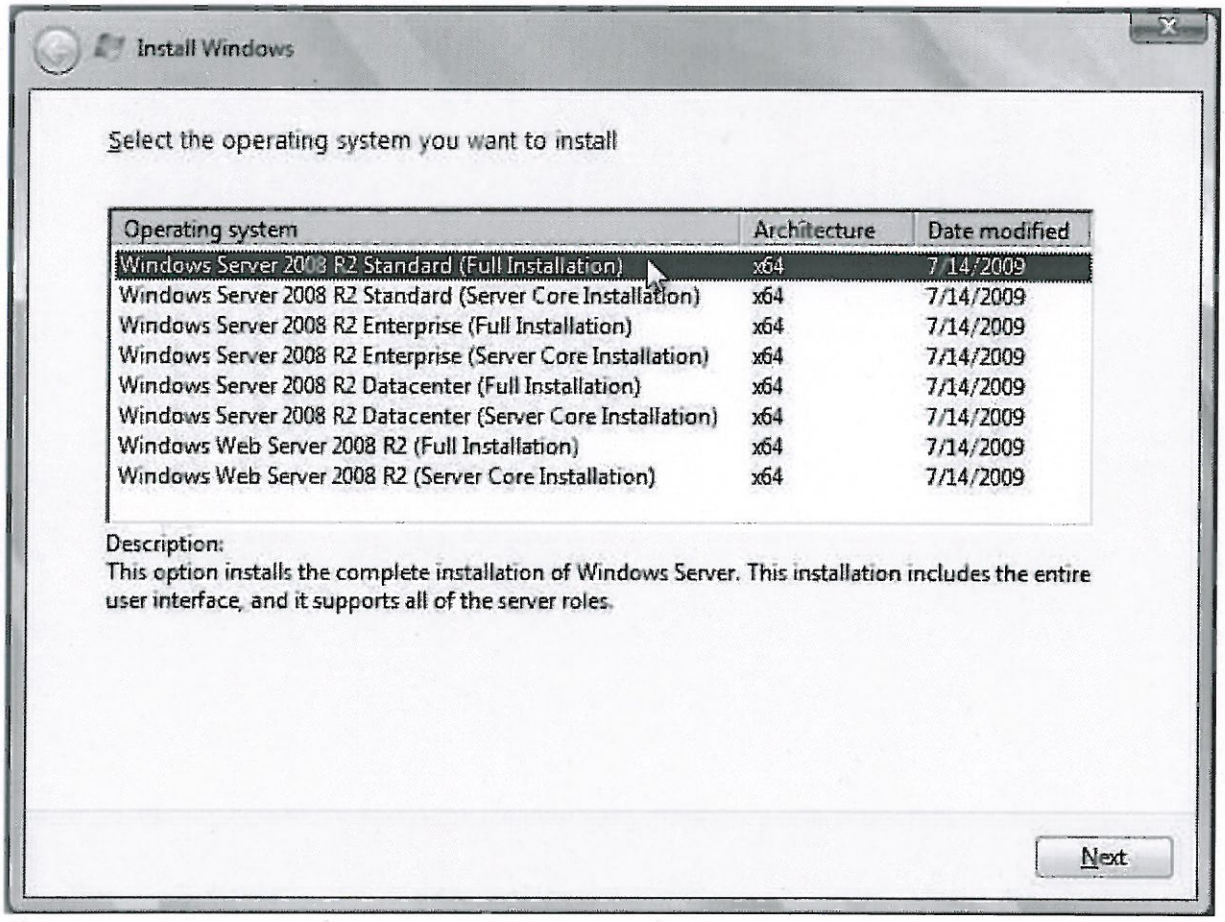
07/12/2016 7/12/2016 07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 5: Select the Operating System you want to install

Select Windows Server 2008 R2 Standard (Full Installation) X64. Page (1/1).

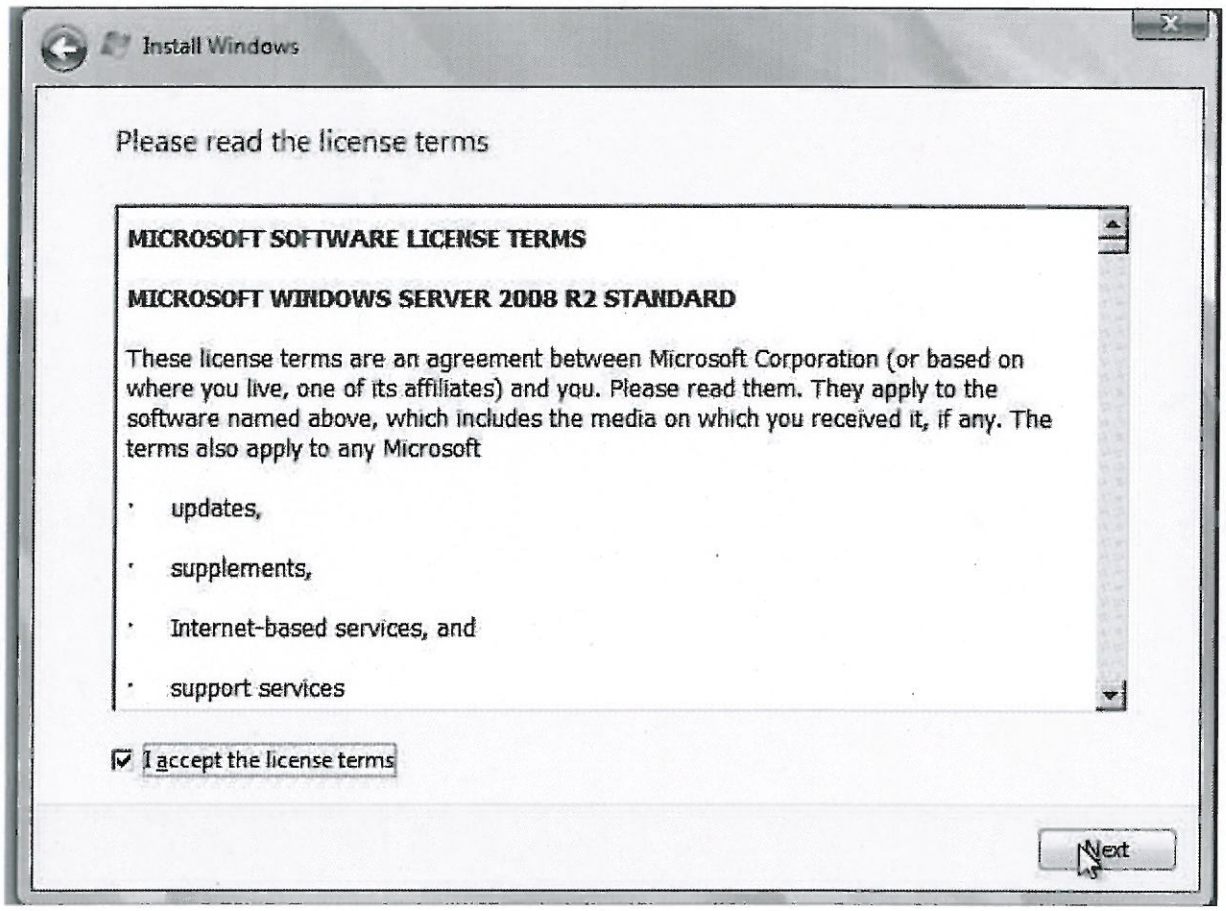


07/12/2016 7/12/2016 07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 6: Read and accept the license terms by clicking to select the checkbox and pressing Next. Page (1/1).

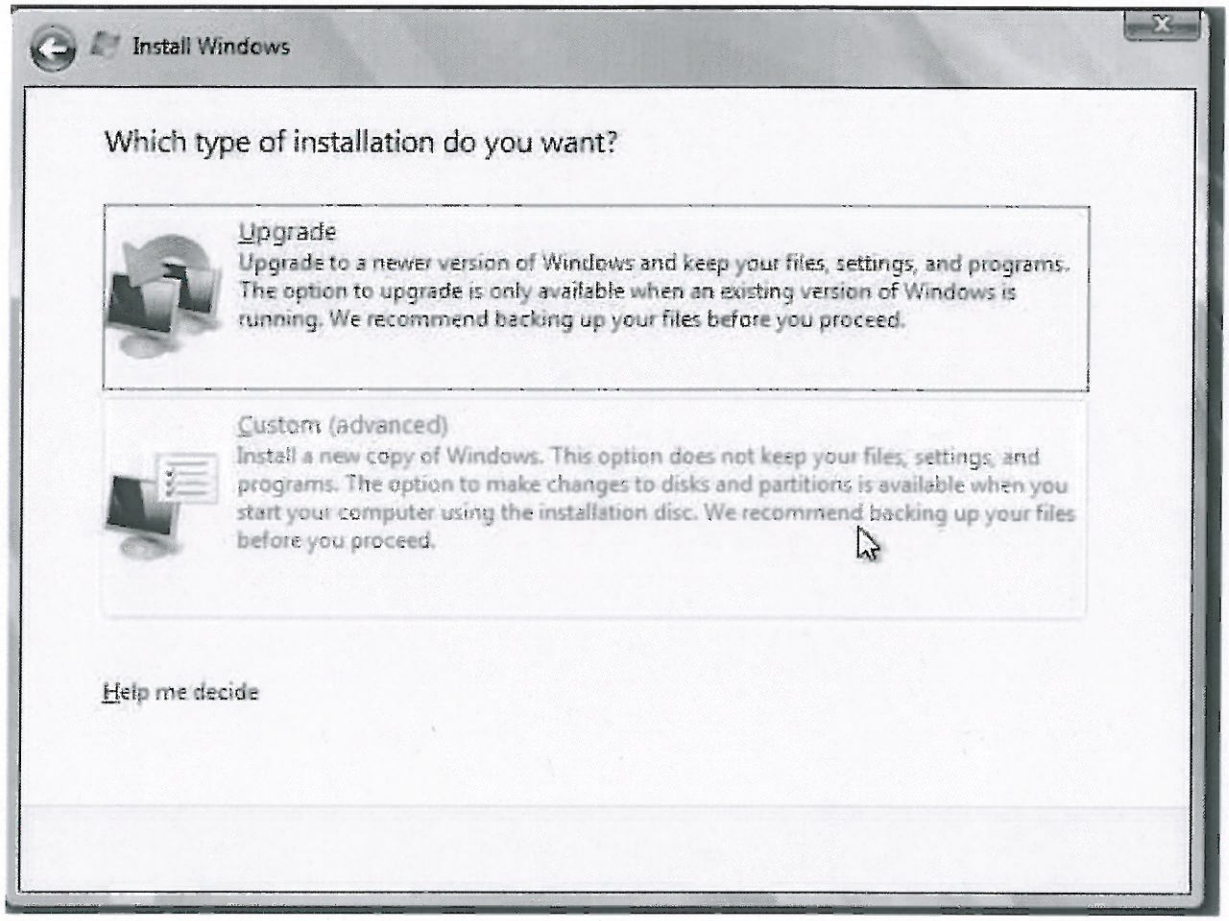


07/12/2016 7/12/2016 07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 7: In the "Which type of installation do you want?" window, click the only available option – Custom (Advanced). Page (1/1).

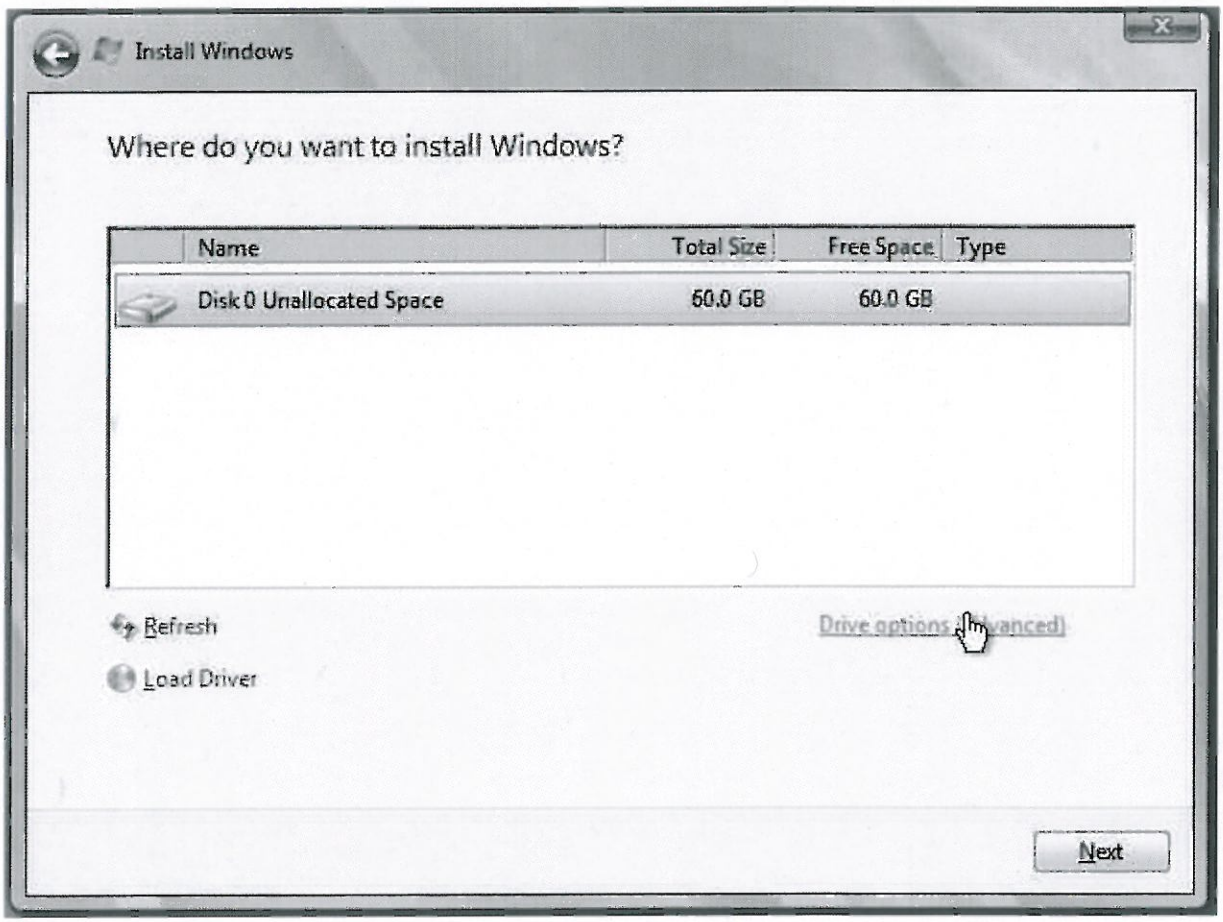


07/12/2016 7/12/2016 07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 8: In the "Where do you want to install Windows?", if you're installing the server on a regular IDE hard disk, click to select the first disk, usually Disk 0, and click Next. Page (1/1).

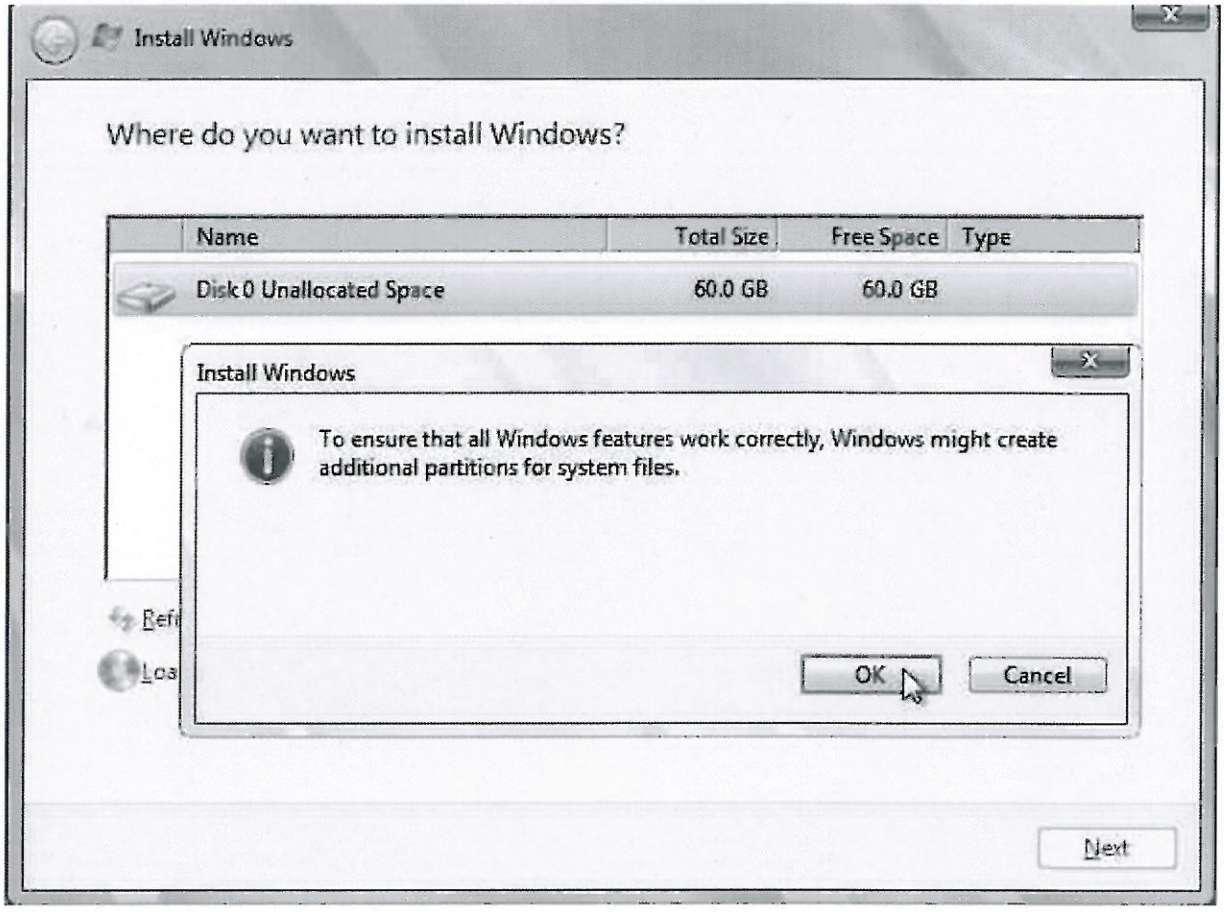


07/12/2016 7/12/2016 07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 9: Where do you want to install windows. Clicked Ok. Page (1/2).

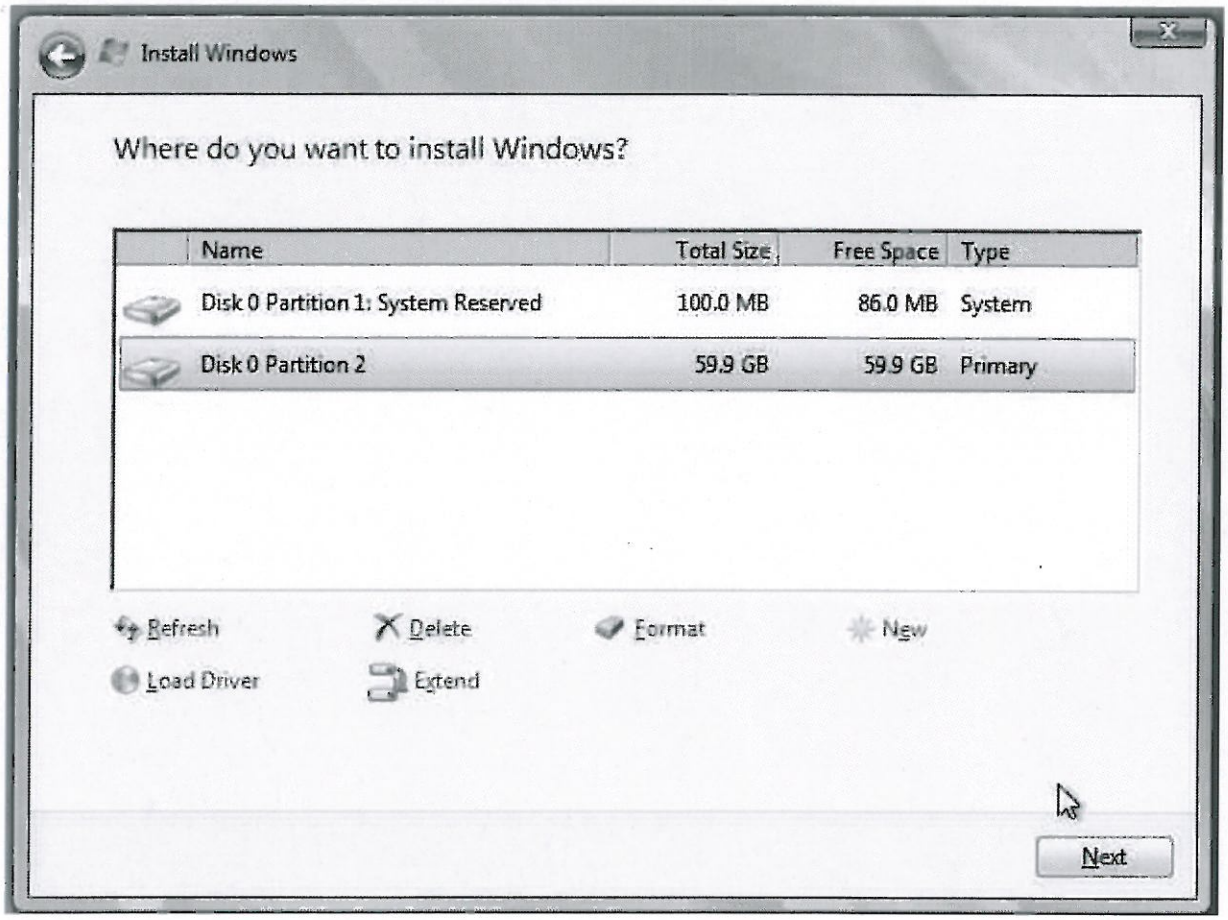


07/12/2016 7/12/2016 07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 9: Selected Disk 0 Partition 2. Page (2/2).

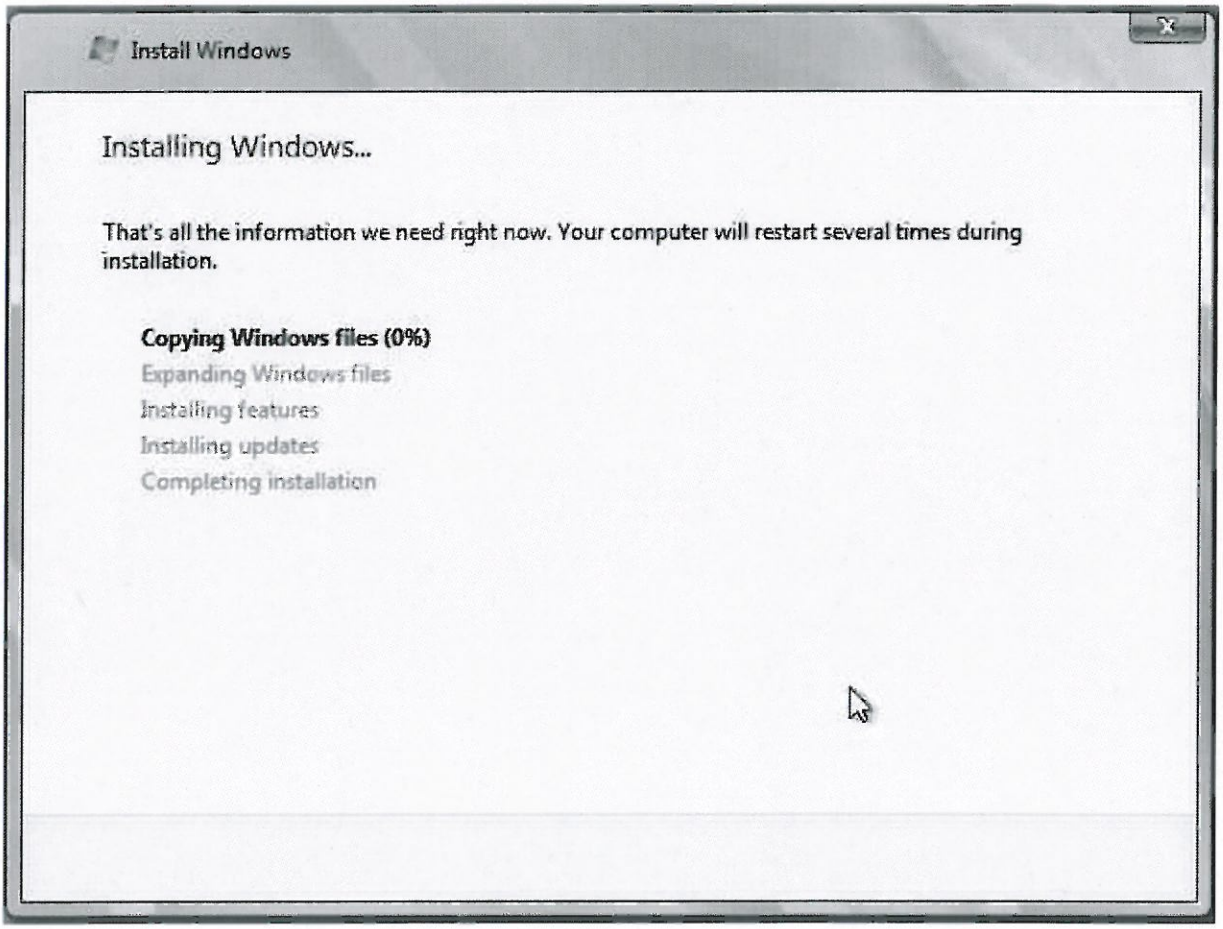


07/12/2016 7/12/2016 07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 10: Installing Windows. Page (1/1).

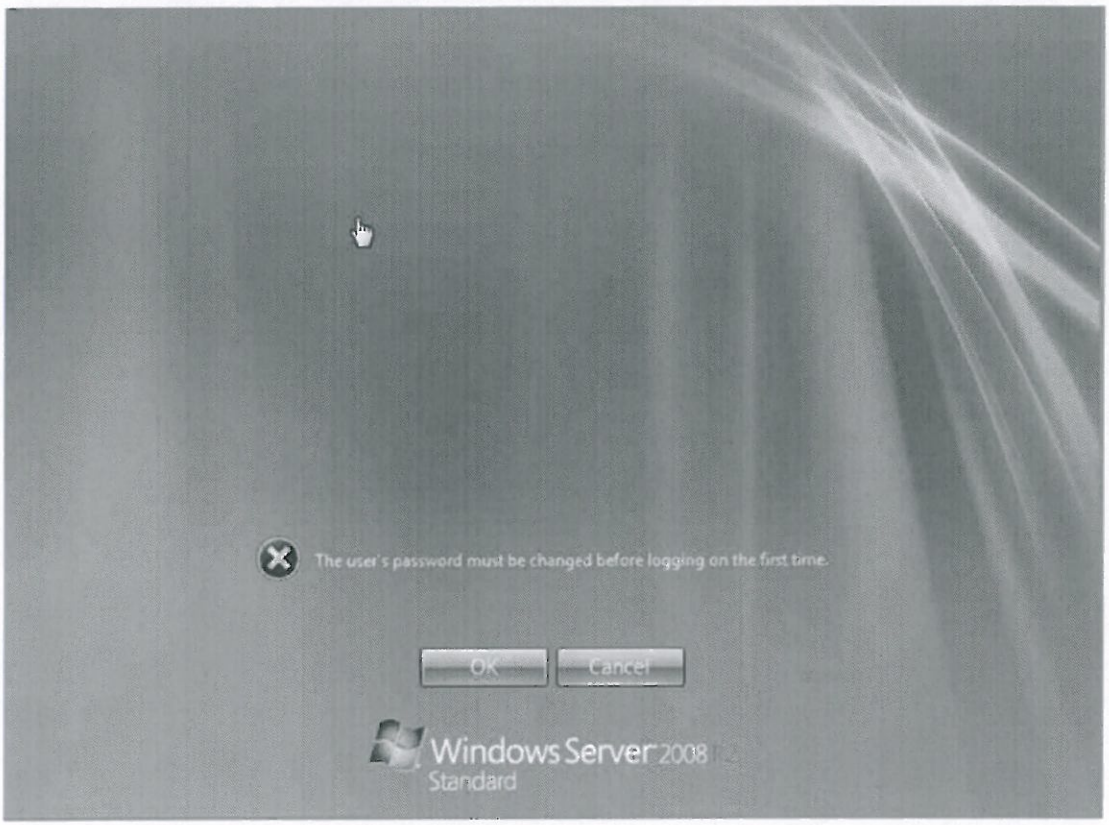


07/12/2016 7/12/2016 07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 11: Then the server reboots prompt with the new Windows Server 2008 type of login screen. Press CTRL+ALT+DEL to log in. Page (1/6).



07/12/2016

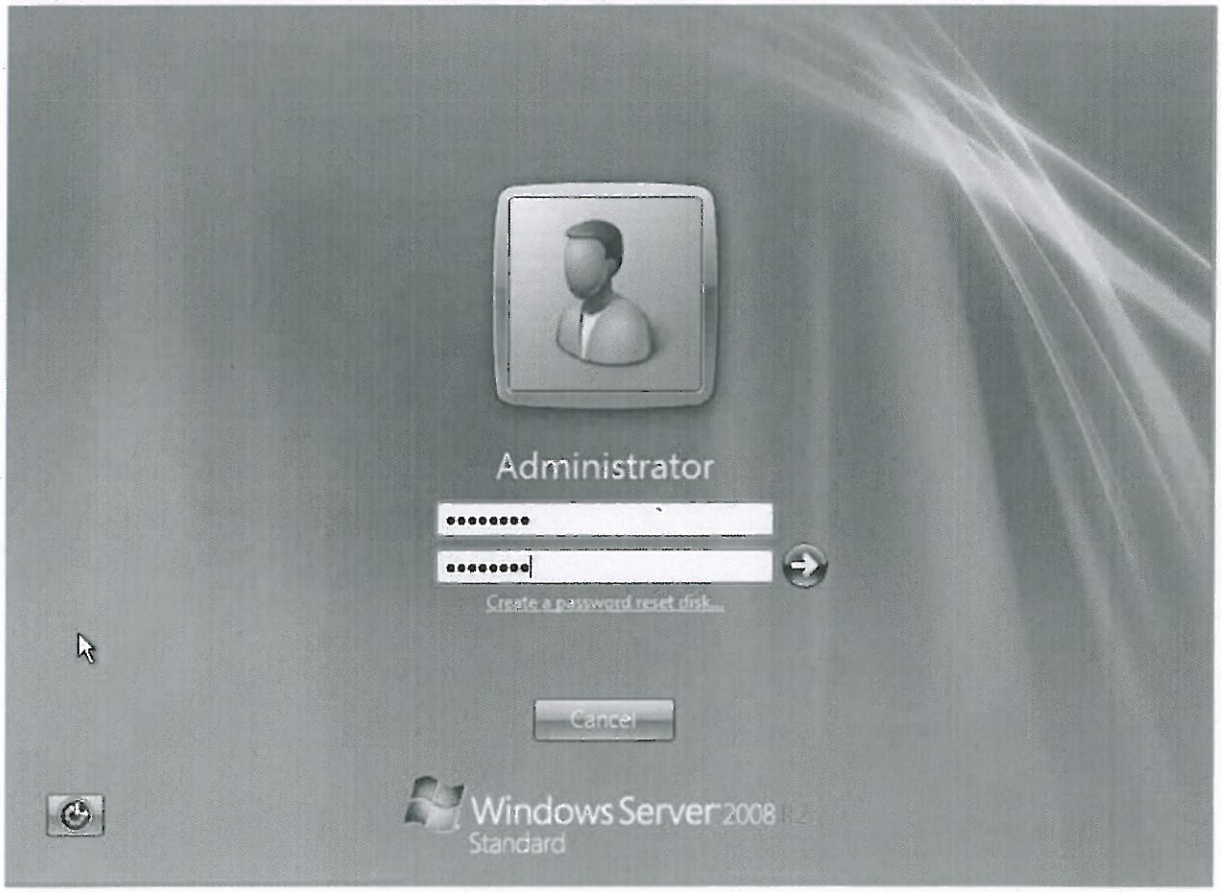
7/12/2016

07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 11: Entered username and password. Page (2/6).

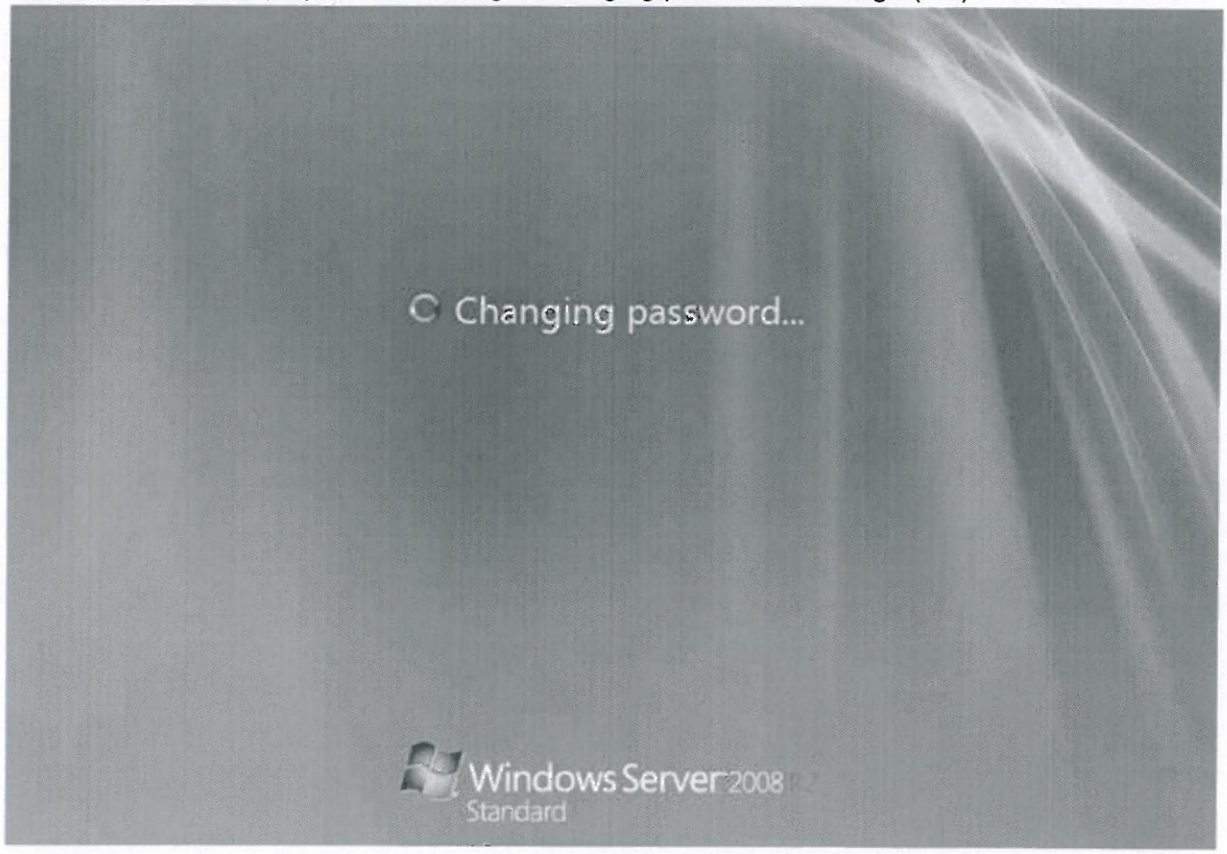


07/12/2016 07/12/2016 07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 11: System displayed the message 'Changing password…'. Page (3/6).



07/12/2016

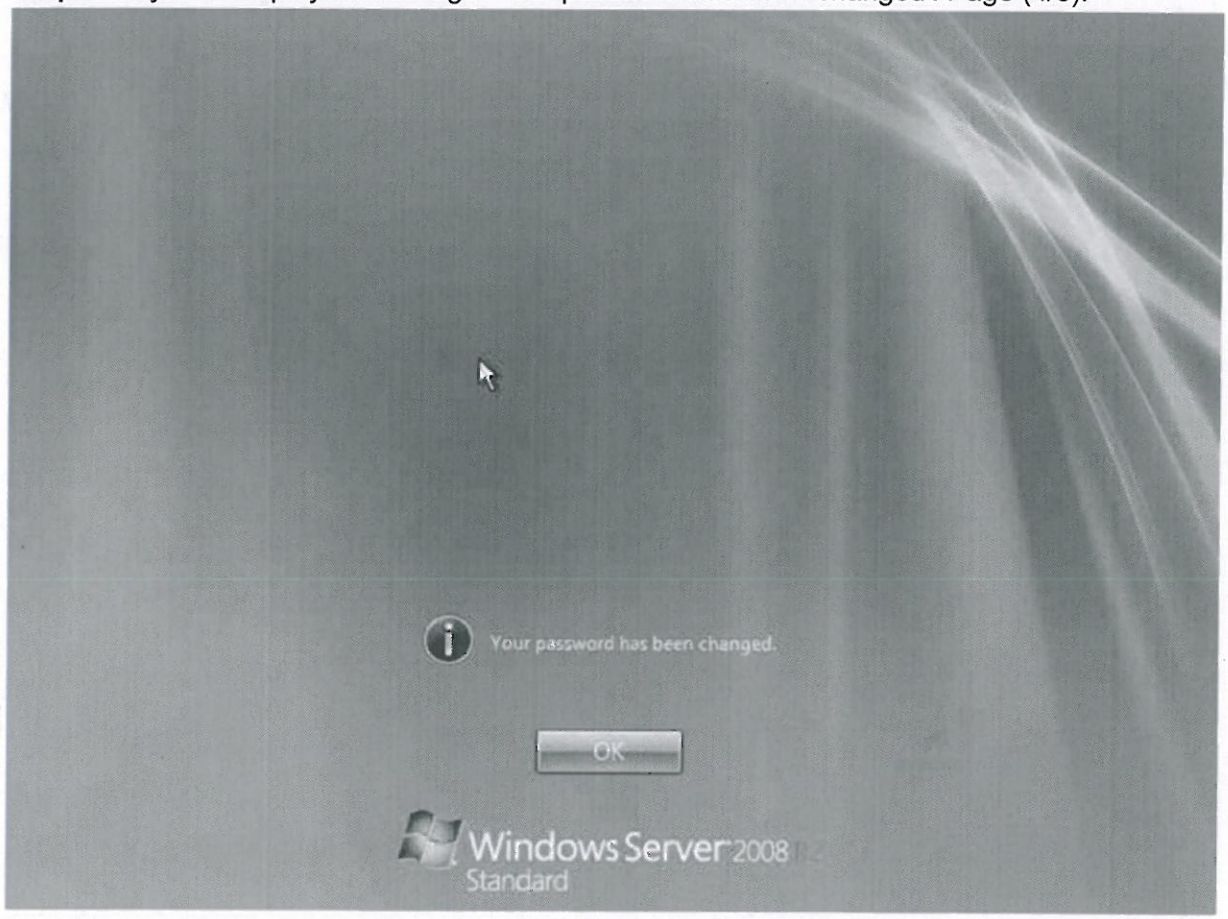
7/12/2016

07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 11: System displayed message 'Your password has been changed'. Page (4/6).



07/12/2016 7/12/2016 07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 11: Continuation… Page (5/6).

07/12/2016

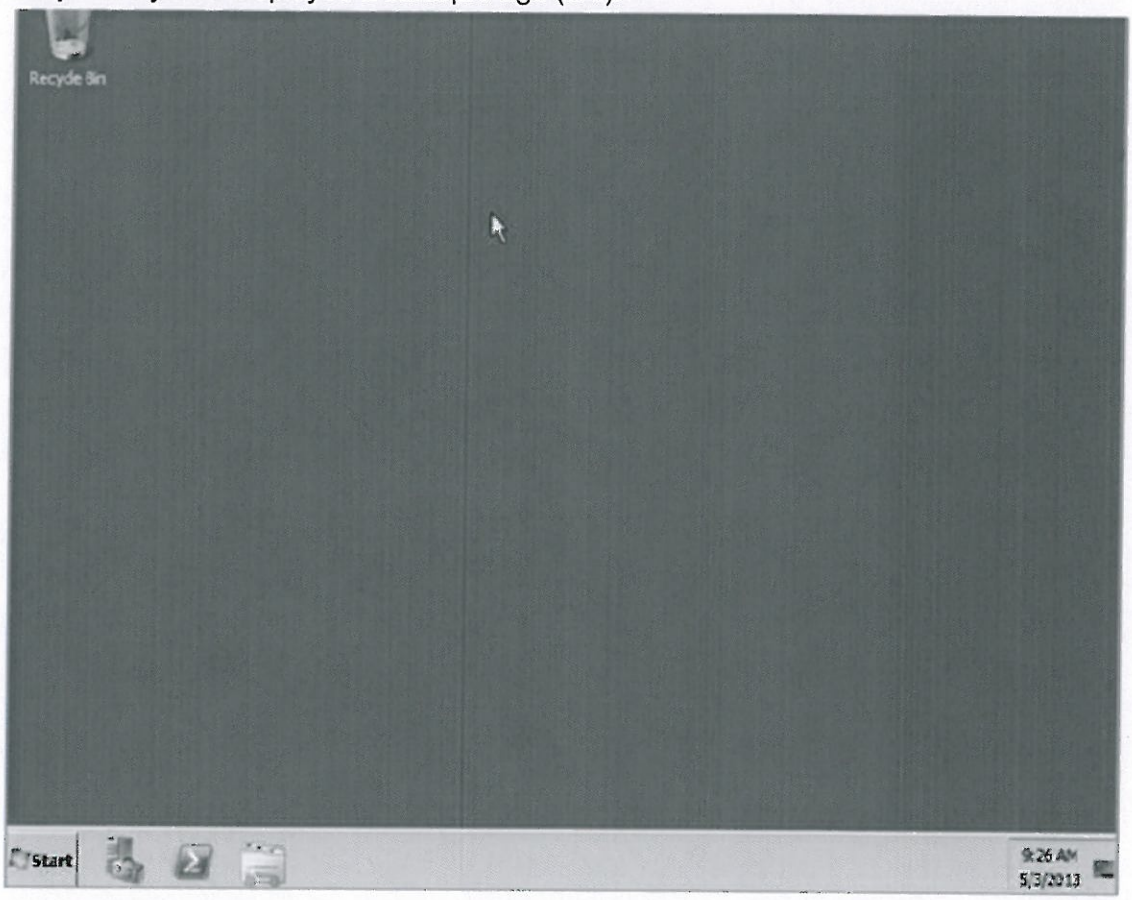
7/12/2016

07/12/2016

Annexure 1
SOP No.: ITP-018

INSTALLATION OF ACTIVE DIRECTORY SERVICES AND LAN SECURITY SERVICES

Step 11: System displayed Desktop. Page (6/6).



07/12/2016

7/12/2016

07/12/2016

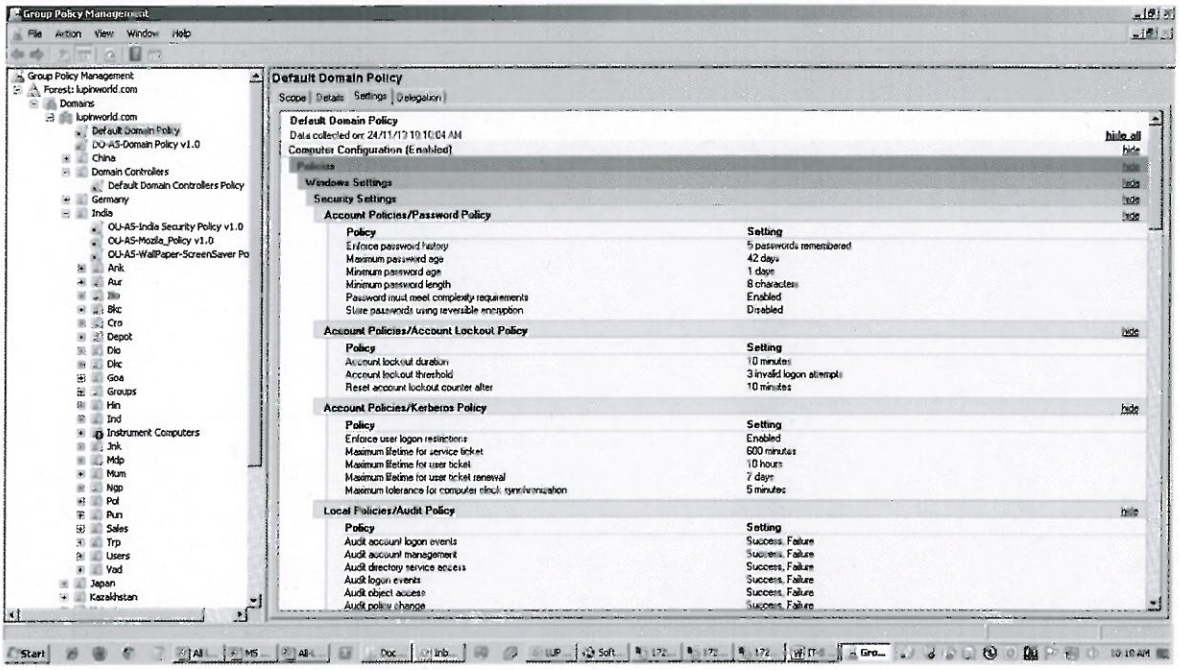
Annexure 2
SOP No.: ITP-018
WINDOW'S XP AND WINDOW 7 SERVICES RUNNING ON LOCAL DESKTOP LAPTOP

Sr. No	Service	Setting (Windows XP)	Setting (Windows 7)
1	Application Layer Gateway Service	Manual	Manual
2	Application Management	Manual	Disable
3	Background Intelligent Transfer Service	Automatic	Manual
4	COM+ Event System	Automatic	Automatic
5	COM+ System Application	Manual	Manual
6	Computer Browser	Manual	Manual
7	Cryptographic Services	Automatic	Automatic
8	DCOM Server Process Launcher	Automatic	Automatic
9	DHCP Client	Automatic	Automatic
10	Distributed Link Tracking Client	Manual	Manual
11	Distributed Transaction Coordinator	Disable	Manual
12	DNS Client	Automatic	Automatic
13	Human Interface Device Access	Manual	Manual
14	Netlogon	Automatic	Disable
15	Network Connections	Automatic	Manual
16	Plug and Play	Manual	Automatic
17	Print Spooler	Manual	Manual
18	Protected Storage	Automatic	Manual
19	Remote Access Auto Connection Manager	Disable	Manual
20	Remote Access Connection Manager	Manual	Manual
21	Remote Procedure Call (RPC)	Automatic	Automatic
22	Remote Procedure Call (RPC) Locator	Manual	Disable
23	Remote Registry	Manual	Disable
24	Routing and Remote Access	Disable(if VPN nt in use)	Disable
25	Secondary Logon	Manual	Manual
26	Security Accounts Manager	Automatic	Automatic
27	Server	Automatic	Automatic
28	Shell Hardware Detection	Automatic	Automatic
29	Smart Card	Disable	Disable
30	Task Scheduler	Manual	Automatic
31	TCP/IP NetBIOS Helper	Manual	Automatic
32	Telephony	Disable	Manual
33	Terminal Services	Disable	Manual
34	Themes	Automatic	Automatic
35	Volume Shadow Copy	Manual	Manual
36	WebClient	Manual	Manual
37	Windows Audio	Automatic	Automatic
38	Windows Installer	Manual	Manually
39	Windows Management Instrumentation	Automatic	Automatic
40	Windows Time	Automatic	Manual

07/12/2016 7/12/2016 07/12/2016

Annexure 3
SOP No.: ITP-018
GROUP POLICY SETTING FOR DATE & TIME

Step1: Password Policy for all locations. Page (1/1).



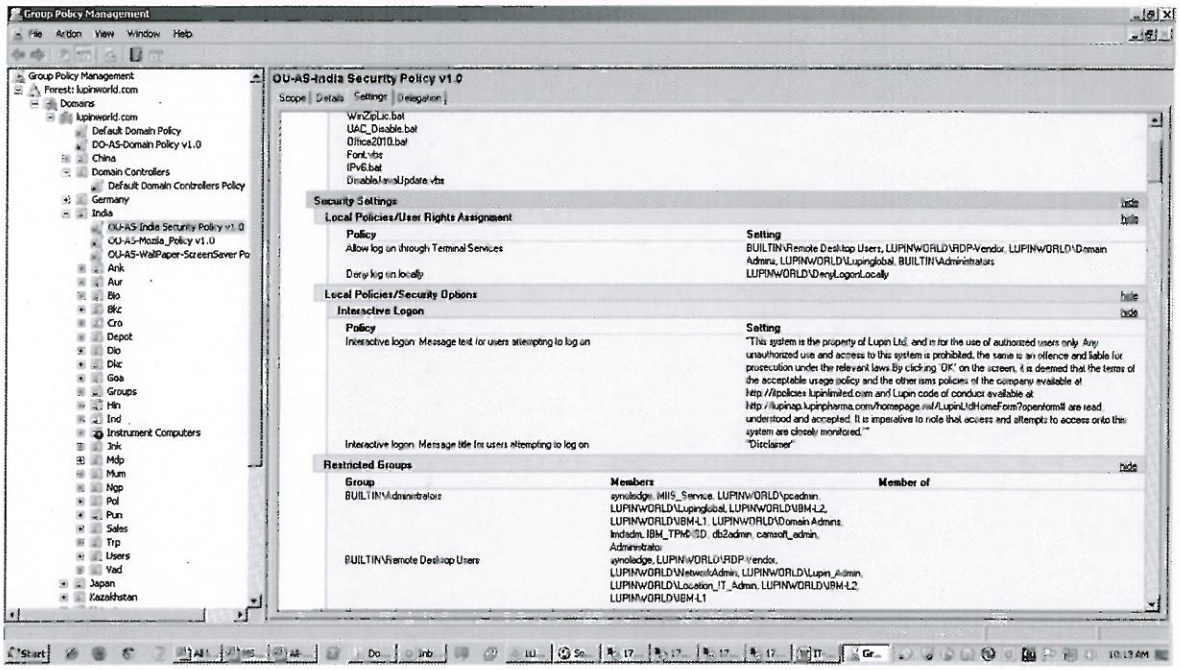
07/12/2016

7/12/2016

07/12/2016

Annexure 3
SOP No.: ITP-018
GROUP POLICY SETTING FOR DATE & TIME

Step2: Local system Policy to apply Date and time format. Page (1/5).



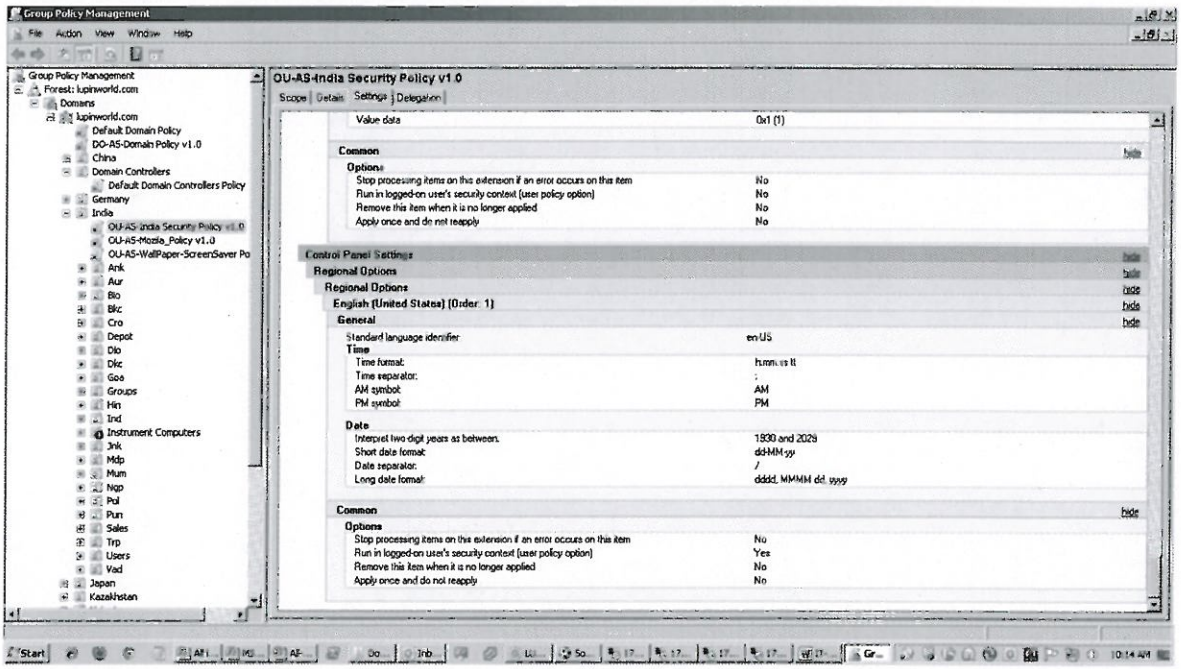
07/12/2016

7/12/2016

07/12/2016

Annexure 3
SOP No.: ITP-018
GROUP POLICY SETTING FOR DATE & TIME

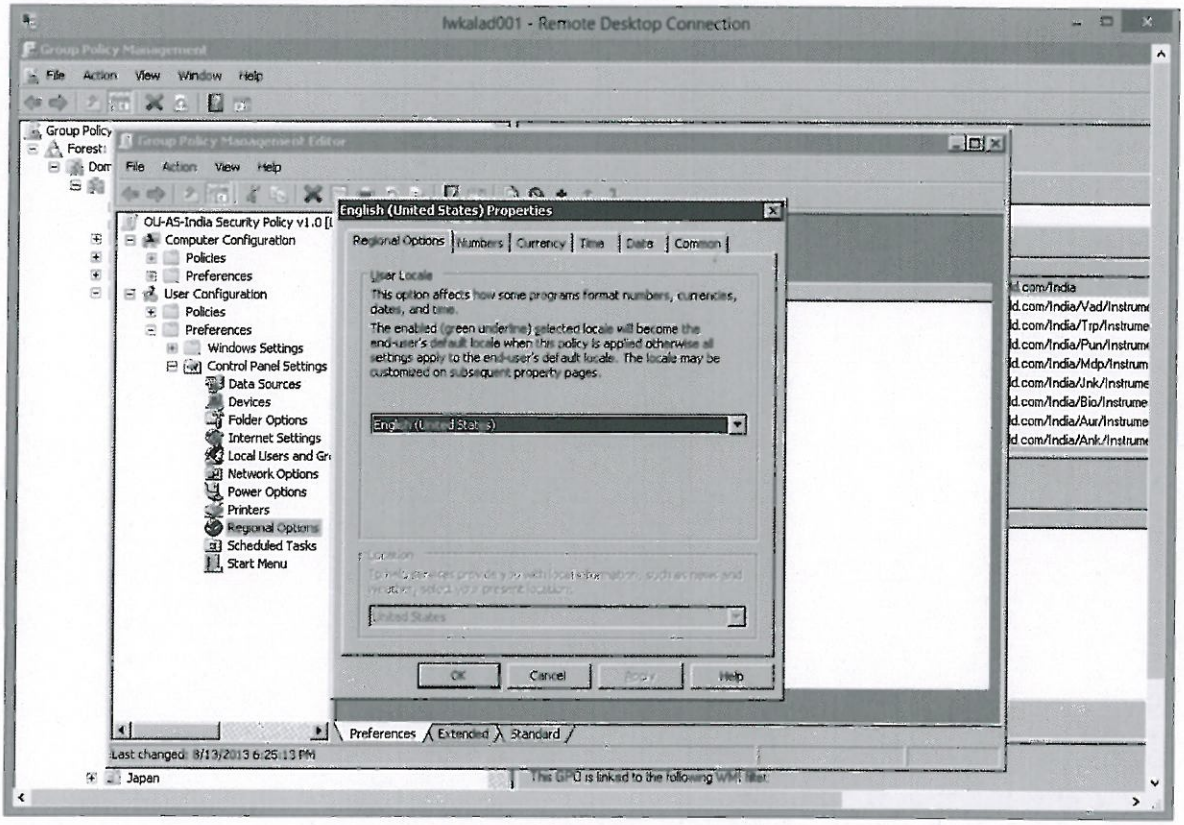
Step2: Local system Policy to apply Date and time format. Page (2/5).



07/12/2016 7/12/2016 07/12/2016

Annexure 3
SOP No.: ITP-018
GROUP POLICY SETTING FOR DATE & TIME

Step 2: Settings done as below. Page (3/5)



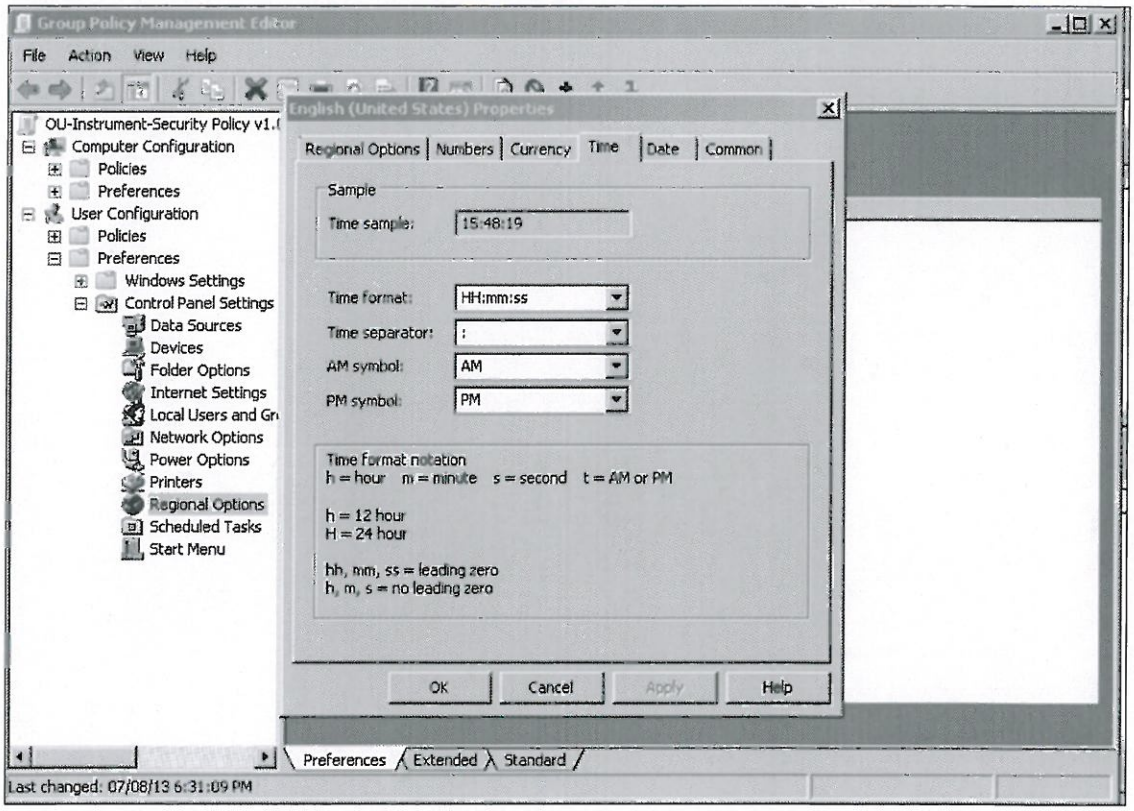
07/12/2016

7/12/2016

07/12/2016

Annexure 3
SOP No.: ITP-018
GROUP POLICY SETTING FOR DATE & TIME

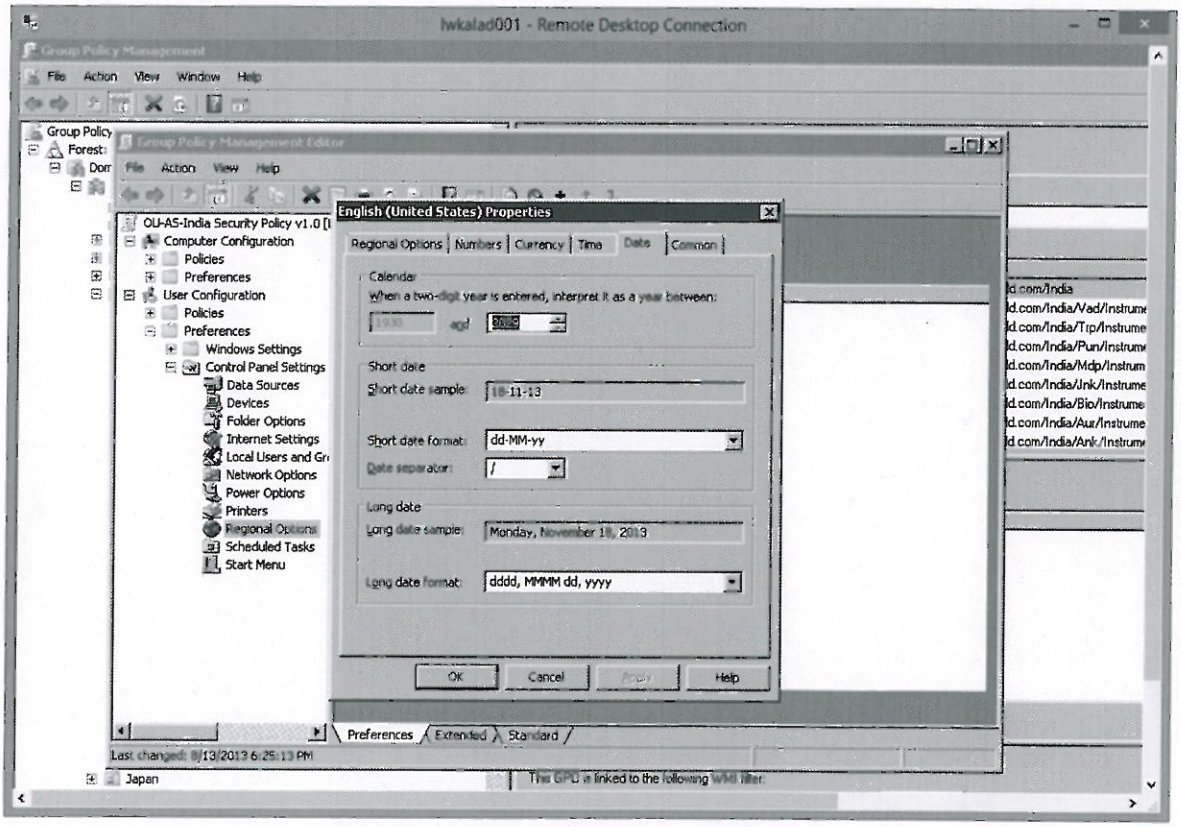
Step 2: Settings done as below. Page (4/5).



07/12/2016 7/12/2016 07/12/2016

Annexure 3
SOP No.: ITP-018
GROUP POLICY SETTING FOR DATE & TIME

Step 5: Settings done as below. Page (5/5).



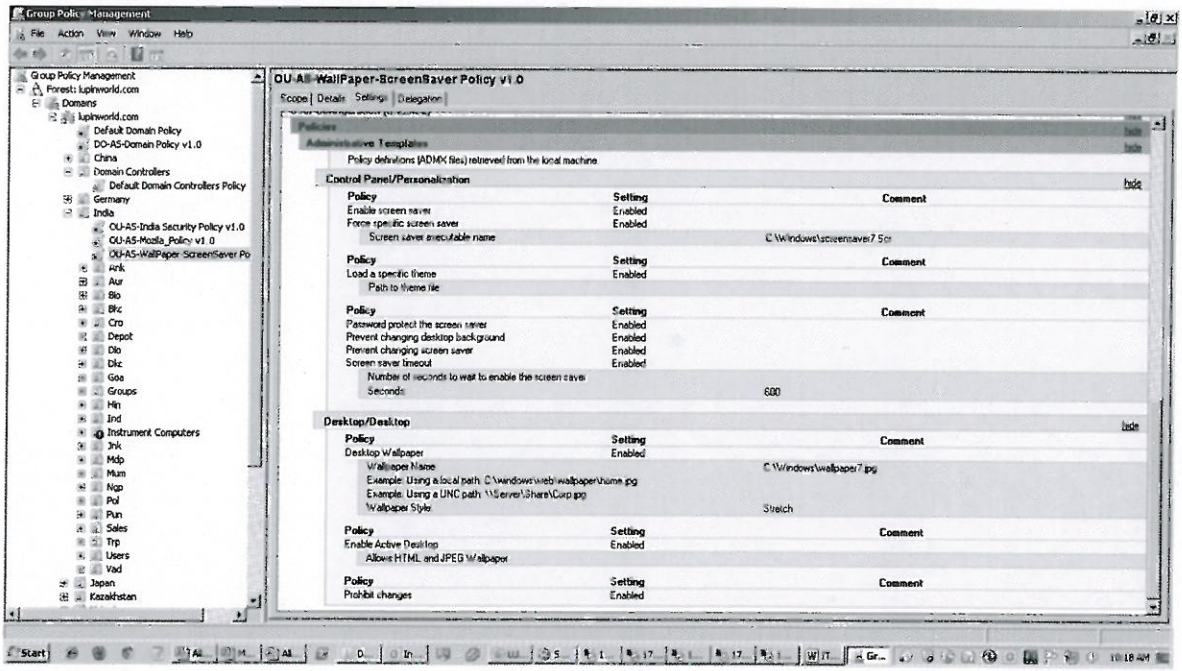
07/12/2016

7/12/2016

07/12/2016

Annexure 3
SOP No.: ITP-018
GROUP POLICY SETTING FOR DATE & TIME

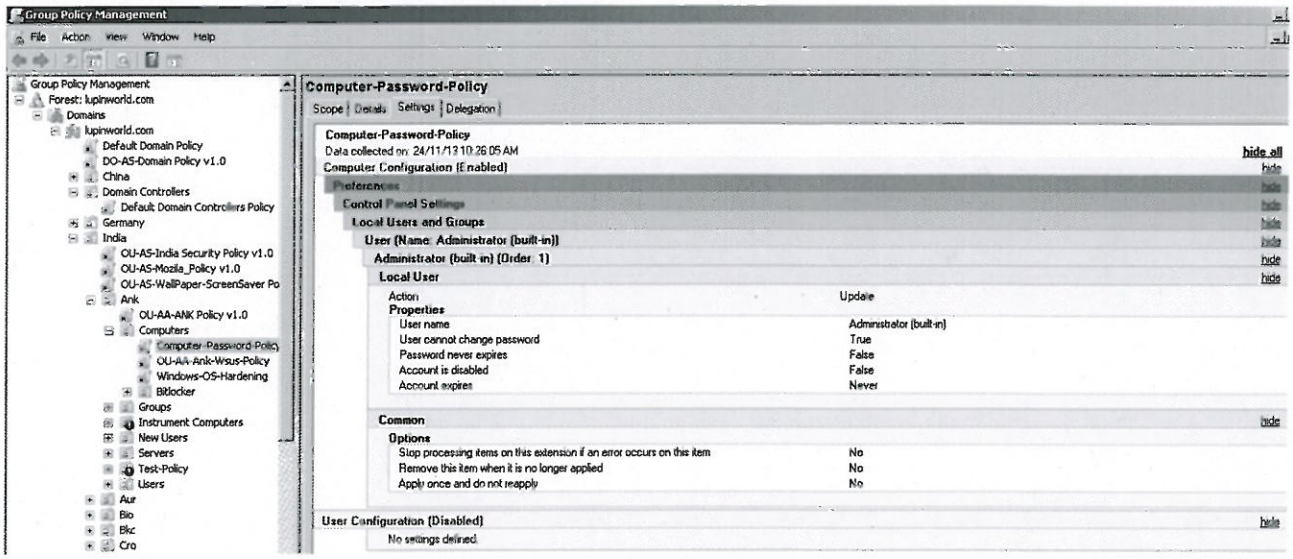
Step3: Central Wallpaper and screen Saver Policy (These changes as and when required). Page (1/1).



07/12/2016 7/12/2016 07/12/2016

Annexure 3
SOP No.: ITP-018
GROUP POLICY SETTING FOR DATE & TIME

Step4: Local Administrator password change policy. Page (1/1).



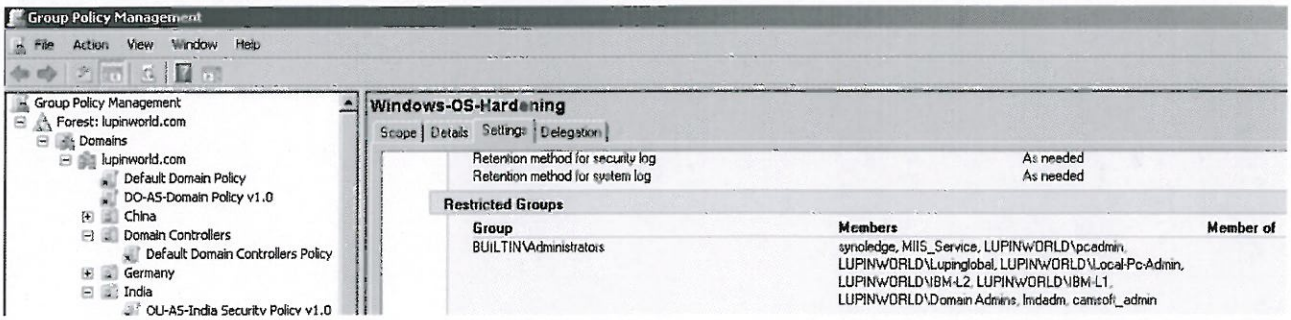
07/12/2016

7/12/2016

07/12/2016

Annexure 3
SOP No.: ITP-018
GROUP POLICY SETTING FOR DATE & TIME

Step5: Build in Administrator policy. Page (1/1).



07/12/2016

7/12/2016

07/12/2016