



Microsoft Active Directory As Built Report

Zen Pr Solutions

Author: Jonathan Colon
Date: Tuesday, March 14, 2023
Version: 1.0

Table of Contents

1 PHARMAX.LOCAL Active Directory Report.....	5
1.1 Forest Information.....	5
1.1.1 Optional Features.....	5
1.1.2 Domain Sites.....	6
1.1.2.1 Site Subnets.....	6
1.1.2.2 Site Links.....	6
1.2 Active Directory Domain Information.....	7
1.2.1 PHARMAX.LOCAL Root Domain Configuration.....	7
1.2.1.1 Flexible Single Master Operations (FSMO).....	7
1.2.1.2 Domain and Trusts.....	8
1.2.1.3 User Accounts in Active Directory.....	8
1.2.1.4 Status of Users Accounts.....	8
1.2.1.5 Privileged Group Count.....	9
1.2.1.6 Computer Accounts in Active Directory.....	10
1.2.1.7 Status of Computer Accounts.....	11
1.2.1.8 Operating Systems Count.....	11
1.2.1.9 Default Domain Password Policy.....	12
1.2.1.10 Fined Grained Password Policies.....	13
1.2.1.11 Local Administrator Password Solution.....	13
1.2.1.12 Group Managed Service Accounts (GMSA).....	13
1.2.1.13 Health Checks.....	13
1.2.1.14 Domain Controller Summary.....	17
1.2.1.14.1 Hardware Inventory.....	17
1.2.1.14.2 NTDS Information.....	18
1.2.1.14.3 Time Source Information.....	18
1.2.1.14.4 SRV Records Status.....	18
1.2.1.14.5 Installed Software.....	18
1.2.1.14.6 DC Diagnostic.....	19
1.2.1.14.7 Infrastructure Services Status.....	23
1.2.1.14.8 Sites Replication Connection.....	24
1.2.1.14.9 Sites Replication Status.....	24
1.2.1.14.10 Group Policy Objects Summary.....	25
1.2.1.14.10.1 Central Store Repository.....	26
1.2.1.14.10.2 User Logon/Logoff Script.....	26

Microsoft Active Directory As Built Report - v1.0

1.2.1.14.10.3 Computer Startup/Shutdown Script	26
1.2.1.14.10.4 Unlinked GPO	27
1.2.1.14.10.5 Empty GPOs.....	27
1.2.1.14.10.6 Enforced GPO.....	27
1.2.1.14.11 Organizational Units	27
1.2.1.14.11.1 GPO Blocked Inheritance.....	35
1.3 Domain Name System Summary.....	35
1.3.1 PHARMAX.LOCAL Root Domain DNS Configuration	35
1.3.1.1 Infrastructure Summary	35
1.3.1.1.1 Forwarder Options	35
1.3.1.2 SERVER-DC-01V DNS Zones	36
1.3.1.2.1 Reverse Lookup Zone	36
1.3.1.2.2 Conditional Forwarder.....	36
1.4 Dynamic Host Configuration Protocol Summary.....	37
1.4.1 PHARMAX.LOCAL Root Domain DHCP Configuration	37
1.4.1.1 DHCP Servers In Active Directory.....	37
1.4.1.1.1 Service Database.....	37
1.4.1.1.2 Dynamic DNS credentials.....	37
1.4.1.2 IPv4 Scope Configuration.....	38
1.4.1.2.1 IPv4 Service Statistics	38
1.4.1.2.2 SERVER-DC-01V IPv4 Scopes.....	38
1.4.1.2.2.1 IPv4 Scope Statistics.....	38
1.4.1.2.2.2 IPv4 Network Interface Binding	39
1.4.1.3 IPv6 Scope Configuration.....	39
1.4.1.3.1 IPv6 Service Statistics	39
1.5 Certificate Authority Summary.....	39
1.5.1 Enterprise Root Certificate Authority	40
1.5.2 Enterprise Subordinate Certificate Authority.....	40
1.5.3 pharmax-SERVER-DC-01V-CA Details.....	42
1.5.3.1 Certificate Validity Period	42
1.5.3.2 Access Control List (ACL)	42
1.5.3.2.1 Access Rights	42
1.5.3.3 Cryptography Configuration	42
1.5.3.4 Authority Information Access (AIA).....	43
1.5.3.5 Certificate Revocation List (CRL).....	44

Microsoft Active Directory As Built Report - v1.0

1.5.3.5.1 CRL Validity Period.....	44
1.5.3.5.2 CRL Flags Settings.....	44
1.5.3.5.3 CRL Distribution Point	44
1.5.3.6 AIA and CDP Health Status.....	46
1.5.3.7 Certificate Template Summary.....	47
1.5.3.7.1 Certificate Template In Active Directory.....	48
1.5.3.8 Key Recovery Agent Certificate.....	49
1.5.4 acad-ACADE-DC-01V-CA Details	50
1.5.4.1 Certificate Validity Period.....	50
1.5.4.2 Access Control List (ACL)	50
1.5.4.2.1 Access Rights	50
1.5.4.3 Cryptography Configuration	51
1.5.4.4 Authority Information Access (AIA).....	51
1.5.4.5 Certificate Revocation List (CRL).....	52
1.5.4.5.1 CRL Validity Period.....	53
1.5.4.5.2 CRL Flags Settings.....	53
1.5.4.5.3 CRL Distribution Point	53
1.5.4.6 AIA and CDP Health Status.....	55
1.5.4.7 Certificate Template Summary.....	55
1.5.4.7.1 Certificate Template In Active Directory.....	56
1.5.4.8 Key Recovery Agent Certificate.....	57
1.5.5 pharmax-CAYEY-DC-01V-CA Details	58
1.5.5.1 Certificate Validity Period.....	58
1.5.5.2 Access Control List (ACL)	58
1.5.5.2.1 Access Rights	59
1.5.5.3 Cryptography Configuration	59
1.5.5.4 Authority Information Access (AIA).....	59
1.5.5.5 Certificate Revocation List (CRL).....	60
1.5.5.5.1 CRL Validity Period.....	60
1.5.5.5.2 CRL Flags Settings.....	60
1.5.5.5.3 CRL Distribution Point	61
1.5.5.6 AIA and CDP Health Status.....	62

1 PHARMAX.LOCAL Active Directory Report

The following section provides a summary of the Active Directory Infrastructure configuration for PHARMAX.LOCAL.

1.1 Forest Information.

The Active Directory framework that holds the objects can be viewed at a number of levels. The forest, tree, and domain are the logical divisions in an Active Directory network. At the top of the structure is the forest. A forest is a collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration. The forest represents the security boundary within which users, computers, groups, and other objects are accessible.

Forest Name	pharmax.local
Forest Functional Level	Windows2016Forest
Schema Version	ObjectVersion 88, Correspond to Windows Server 2019
Tombstone Lifetime (days)	180
Domains	acad.pharmax.local; pharmax.local; uia.local
Global Catalogs	Server-DC-01V.pharmax.local; acad-dc-01v.acad.pharmax.local; DC-UIA-01V.uia.local
Domains Count	3
Global Catalogs Count	3
Sites Count	5
Application Partitions	DC=DomainDnsZones,DC=acad,DC=pharmax,DC=local DC=ForestDnsZones,DC=pharmax,DC=local DC=DomainDnsZones,DC=uia,DC=local DC=DomainDnsZones,DC=pharmax,DC=local
PartitionsContainer	CN=Partitions,CN=Configuration,DC=pharmax,DC=local
SPN Suffixes	-
UPN Suffixes	pharmax acad

Table 1 - Forest Summary - PHARMAX.LOCAL

1.1.1 Optional Features

Name	Required Forest Mode	Enabled
Privileged Access Management Feature	Windows2016Forest	No
Recycle Bin Feature	Windows2008R2Forest	Yes

Table 2 - Optional Features - PHARMAX.LOCAL

1.1.2 Domain Sites

Site Name	Description	Subnets	Creation Date
ACAD	-	172.23.4.0/24	9/5/2021
Cayey-Branch	Site of Cayey, PR Branch	10.10.0.0/16	9/3/2021
Dead-Site	-	-	1/22/2022
Pharmax-HQ	Site of San Juan, PR HQ	10.9.1.0/24 192.168.0.0/16	6/10/2018
UIA	-	172.23.7.0/24	5/11/2022

Table 3 - Sites - PHARMAX.LOCAL

Health Check:

Corrective Actions: Ensure Sites have an associated subnet. If subnets are not associated with AD Sites users in the AD Sites might choose a remote domain controller for authentication which in turn might result in excessive use of a remote domain controller.

Best Practices: Ensure Sites have a defined description.

1.1.2.1 Site Subnets

Subnet	Description	Sites	Creation Date
10.10.0.0/16	Cayey-Networks	Cayey-Branch	9/12/2020
10.9.1.0/24	-	Pharmax-HQ	9/14/2021
172.23.4.0/24	-	ACAD	5/11/2022
172.23.7.0/24	-	UIA	5/11/2022
192.168.0.0/16	-	Pharmax-HQ	9/12/2020

Table 4 - Site Subnets - PHARMAX.LOCAL

Health Check:

Best Practices: Ensure that subnets has a defined description.

1.1.2.2 Site Links

Site Link Name	Cost	Replication Frequency	Transport Protocol	Sites
PHARMAX-to-ACAD	100	15 min	IP	ACAD Pharmax-HQ
Pharmax-to-All	100	15 min	IP	UIA Dead-Site ACAD Cayey-Branch Pharmax-HQ

Table 5 - Site Links - PHARMAX.LOCAL

1.2 Active Directory Domain Information

An Active Directory domain is a collection of objects within a Microsoft Active Directory network. An object can be a single user or a group or it can be a hardware component, such as a computer or printer. Each domain holds a database containing object identity information. Active Directory domains can be identified using a DNS name, which can be the same as an organization's public domain name, a sub-domain or an alternate version (which may end in .local).

1.2.1 PHARMAX.LOCAL Root Domain Configuration

The following section provides a summary of the Active Directory Domain Information.

Domain Name	pharmax
NetBIOS Name	PHARMAX
Domain SID	S-1-5-21-2867495315-1194516362-180967319
Domain Functional Level	Windows2016Domain
Domains	-
Forest	pharmax.local
Parent Domain	-
Replica Directory Servers	Server-DC-01V.pharmax.local cayey-dc-01v.pharmax.local
Child Domains	acad.pharmax.local
Domain Path	pharmax.local/
Computers Container	pharmax.local/Computers
Domain Controllers Container	pharmax.local/Domain Controllers
Systems Container	pharmax.local/System
Users Container	pharmax.local/Users
ReadOnly Replica Directory Servers	-
ms-DS-MachineAccountQuota	10
RID Issued	8100
RID Available	1073733723

Table 6 - Domain Summary - PHARMAX.LOCAL

1.2.1.1 Flexible Single Master Operations (FSMO)

Infrastructure Master Server	Server-DC-01V.pharmax.local
RID Master Server	Server-DC-01V.pharmax.local
PDC Emulator Name	Server-DC-01V.pharmax.local
Domain Naming Master Server	Server-DC-01V.pharmax.local
Schema Master Server	Server-DC-01V.pharmax.local

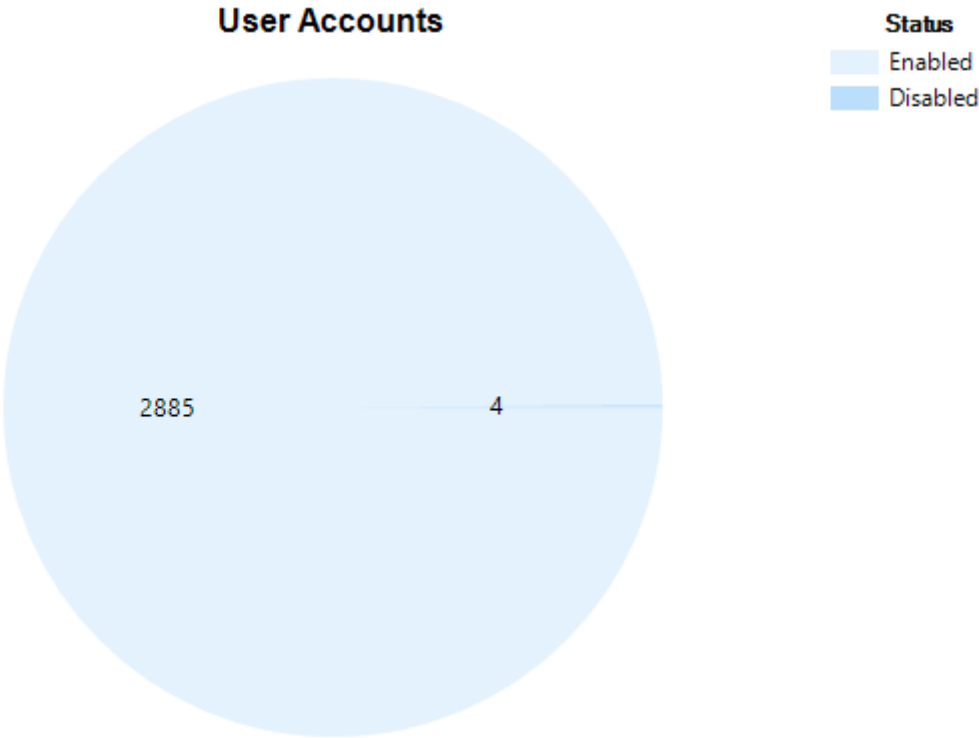
Table 7 - FSMO Server - pharmax.local

1.2.1.2 Domain and Trusts

Name	Path	Source	Target	Direction
acad.pharmax.local	pharmax.local/System/acad.pharmax.local	pharmax	acad.pharmax.local	BiDirectional
uia.local	pharmax.local/System/uia.local	pharmax	uia.local	BiDirectional

Table 8 - Trusts - PHARMAX.LOCAL

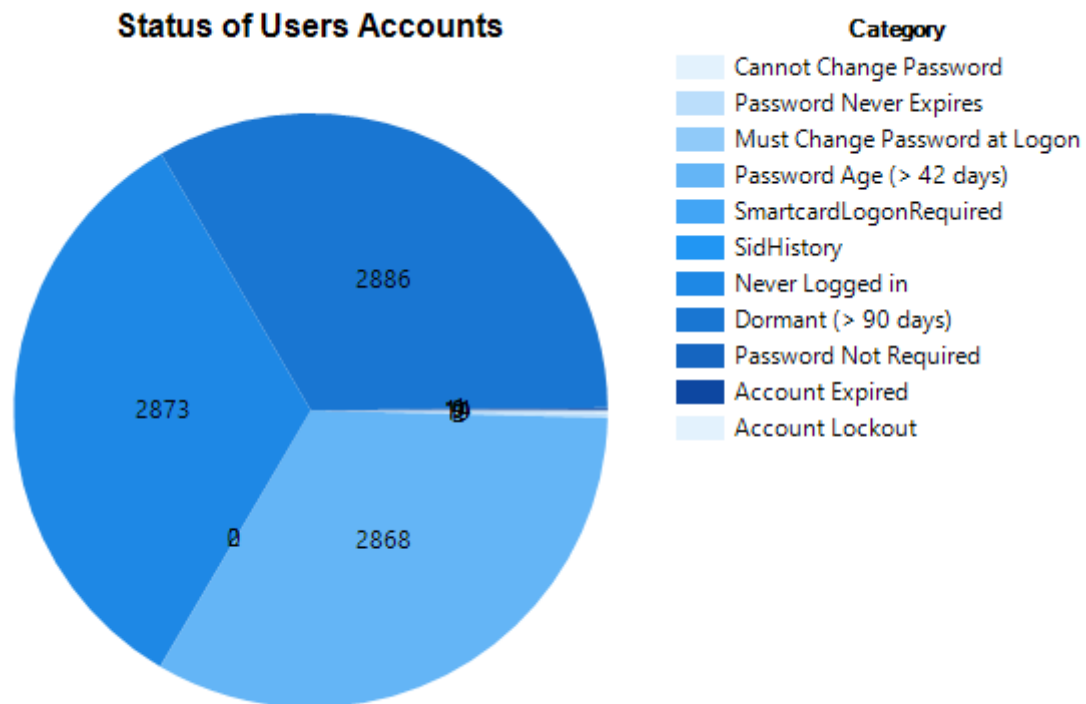
1.2.1.3 User Accounts in Active Directory



Status	Count	Percentage
Enabled	2885	100%
Disabled	4	0%

Table 9 - User Accounts in Active Directory - PHARMAX.LOCAL

1.2.1.4 Status of Users Accounts



Category	Enabled Count	Enabled %	Disabled Count	Disabled %	Total Count	Total %
Cannot Change Password	14	0	1	0	14	0
Password Never Expires	19	1	1	0	19	1
Must Change Password at Logon	2	0	1	0	2	0
Password Age (> 42 days)	2868	99	1	0	2868	99
SmartcardLogonRequired	2	0	1	0	2	0
SidHistory	0	0	1	0	0	0
Never Logged in	2873	99	1	0	2873	99
Dormant (> 90 days)	2886	100	1	0	2886	100
Password Not Required	4	0	1	0	4	0
Account Expired	9	0	1	0	9	0
Account Lockout	0	0	1	0	0	0

Table 10 - Status of User Accounts - PHARMAX.LOCAL

1.2.1.5 Privileged Group Count

Group Name	Count
Account Operators	1
Administrators	6
Backup Operators	2

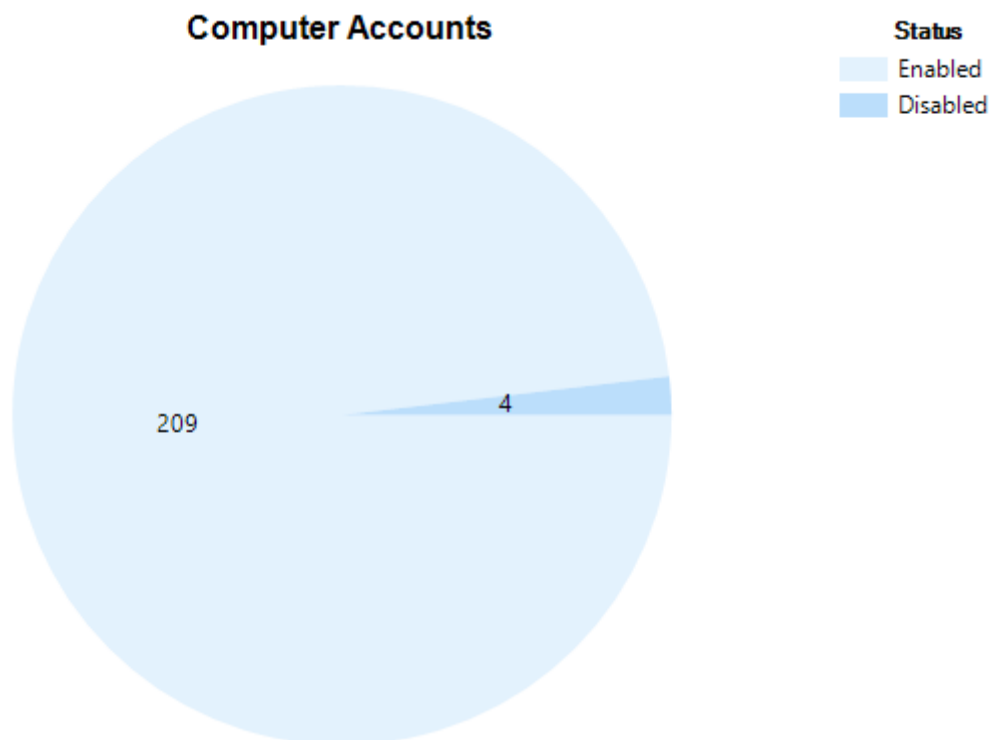
Group Name	Count
Cert Publishers	4
DnsAdmins	3
Domain Admins	5
Enterprise Admins	2
Incoming Forest Trust Builders	2
Key Admins	2
Print Operators	1
Remote Desktop Users	3
Schema Admins	25
Server Operators	3

Table 11 - Privileged Group Count - PHARMAX.LOCAL

Health Check:

Security Best Practice: The Schema Admins group is a privileged group in a forest root domain. Members of the Schema Admins group can make changes to the schema, which is the framework for the Active Directory forest. Changes to the schema are not frequently required. This group only contains the Built-in Administrator account by default. Additional accounts must only be added when changes to the schema are necessary and then must be removed.

1.2.1.6 Computer Accounts in Active Directory

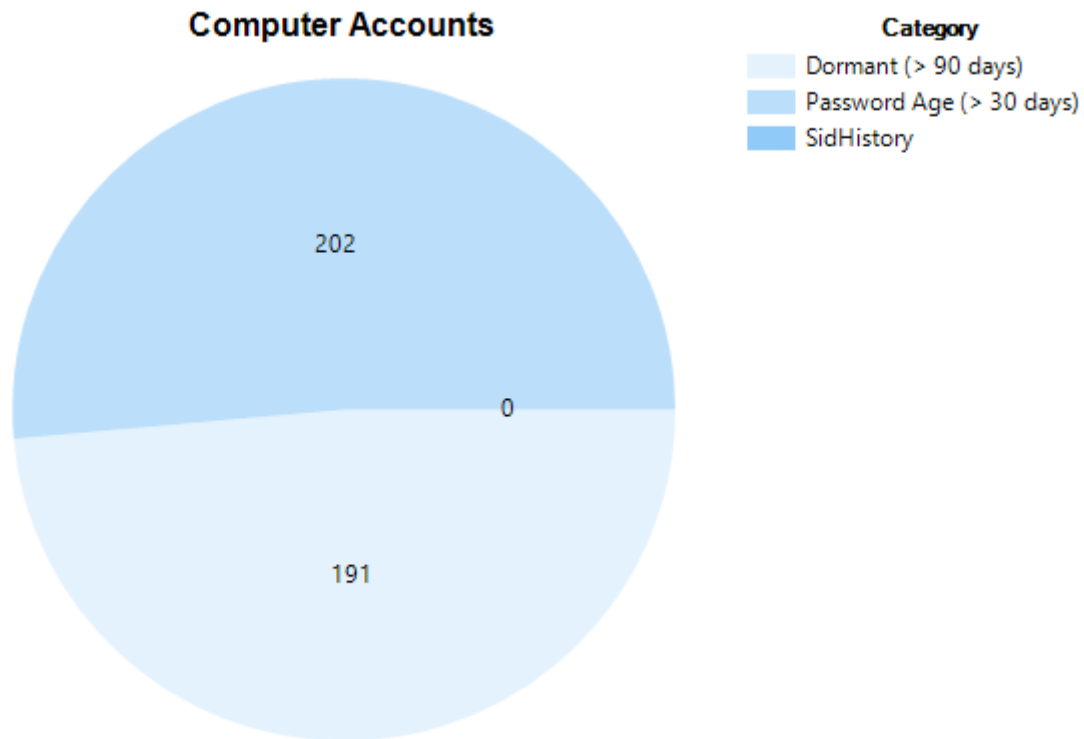


Microsoft Active Directory As Built Report - v1.0

Status	Count	Percentage
Enabled	209	98%
Disabled	4	2%

Table 12 - Computer Accounts in Active Directory - PHARMAX.LOCAL

1.2.1.7 Status of Computer Accounts



Category	Enabled Count	Enabled %	Disabled Count	Disabled %	Total Count	Total %
Dormant (> 90 days)	191	90	1	0	191	90
Password Age (> 30 days)	202	95	1	0	202	95
SidHistory	0	0	1	0	0	0

Table 13 - Status of Computer Accounts - PHARMAX.LOCAL

1.2.1.8 Operating Systems Count

Operating System	Count
CentOS	1
Data Domain OS	1
EMC File Server	1
NetApp Release 9.5P6	1

Microsoft Active Directory As Built Report - v1.0

Operating System	Count
NetApp Release 9.8	1
NetApp Release 9.8P7	1
NetApp Release 9.9.1P1	3
OneFS	1
redhat-linux-gnu	1
unknown	7
Unknown	103
Windows 10 Education	1
Windows 10 Enterprise	1
Windows 10 Enterprise Evaluation	19
Windows Server 2003	1
Windows Server 2016 Standard Evaluation	10
Windows Server 2019 Standard	1
Windows Server 2019 Standard Evaluation	44
Windows Server 2022 Datacenter	3
Windows Server 2022 Datacenter Evaluation	10
Windows Vista	1
Windows XP	1

Table 14 - Operating System Count - PHARMAX.LOCAL

Health Check:

Security Best Practice: Operating systems that are no longer supported for security updates are not maintained or updated for vulnerabilities leaving them open to potential attack.

Organizations must transition to a supported operating system to ensure continued support and to increase the organization security posture

1.2.1.9 Default Domain Password Policy

Password Must Meet Complexity Requirements	Yes
Path	pharmax.local/
Lockout Duration	30 minutes
Lockout Threshold	5
Lockout Observation Window	30 minutes
Max Password Age	42 days
Min Password Age	01 days
Min Password Length	7
Enforce Password History	24
Store Password using Reversible Encryption	No

Table 15 - Default Domain Password Policy - PHARMAX.LOCAL

1.2.1.10 Fined Grained Password Policies

Name	Lockout Duration	Max Password Age	Min Password Age	Min Password Length	Password History Count
Administrators	30 minutes	42 days	05 days	12	90
Test	30 minutes	42 days	01 days	7	23

Table 16 - Fined Grained Password Policies - PHARMAX.LOCAL

1.2.1.11 Local Administrator Password Solution

Name	Domain Name	Enabled
ms-Mcs-AdmPwd	pharmax.local	Yes

Table 17 - Local Administrator Password Solution - PHARMAX.LOCAL

1.2.1.12 Group Managed Service Accounts (GMSA)

Name	SamAccount Name	DNS Host Name	Host Computers	Retrieve Managed Password	Primary Group	Enabled
SQLServer	SQLServer\$	SQL-Cluster	SQL-CLUSTER-02V, SQL-CLUSTER-01V	SQL-CLUSTER-01V, SQL-CLUSTER-02V	Domain Computers	Yes
adfsgmsa	adfsgmsa\$	ADFS.pharmax.local		SERVER-ADFS-01V, SERVER-ADFS-02V	Domain Computers	Yes

Table 18 - Group Managed Service Accounts - PHARMAX.LOCAL

1.2.1.13 Health Checks

Naming Context Last Backup

The following section details naming context last backup time for Domain PHARMAX.LOCAL.

Naming Context	Last Backup	Last Backup in Days
CN=Configuration,DC=pharmax,DC=local	2023:02:20	21
CN=Schema,CN=Configuration,DC=pharmax,DC=local	2023:02:20	21
DC=DomainDnsZones,DC=pharmax,DC=local	2023:02:20	21
DC=ForestDnsZones,DC=pharmax,DC=local	2023:02:20	21

Naming Context	Last Backup	Last Backup in Days
DC=pharmax,DC=local	2023:02:20	21

Table 19 - Naming Context Last Backup - PHARMAX.LOCAL

Health Check:**Corrective Actions: Ensure there is a recent (<180 days) Active Directory backup.**

Sysvol Folder Status

The following section details domain PHARMAX.LOCAL sysvol health status.

Extension	File Count	Size
.aas	3	0.09 MB
.adm	3	0.04 MB
.adml	4684	75.08 MB
.admx	222	3.83 MB
.cmtx	6	0.00 MB
.config	7	0.03 MB
.dll	10	12.22 MB
.exe	18	85.80 MB
.inf	9	0.01 MB
.INI	16	0.01 MB
.msi	3	103.04 MB
.pol	13	0.03 MB
.xml	4	0.01 MB
.zip	5	143.60 MB

Table 20 - Sysvol Folder Status - PHARMAX.LOCAL

Health Check:**Corrective Actions: Make sure Sysvol content has no malicious extensions or unnecessary content.**

Netlogon Folder Status

The following section details domain PHARMAX.LOCAL netlogon health status.

Extension	File Count	Size
.adm	1	0.01 MB
.adml	1	0.03 MB
.admx	1	0.02 MB
.config	7	0.03 MB
.dll	10	12.22 MB
.exe	18	85.80 MB
.ini	1	0.01 MB

Extension	File Count	Size
.msi	3	103.04 MB
.xml	1	0.00 MB
.zip	5	143.60 MB

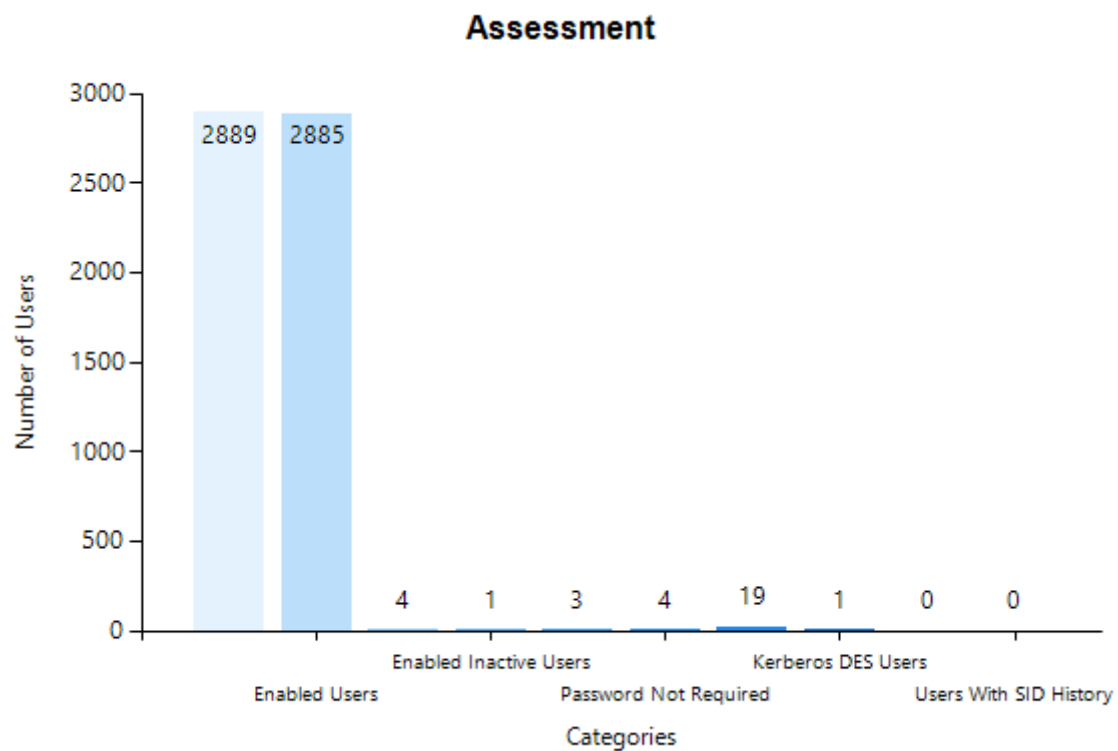
Table 21 - Netlogon Folder Status - PHARMAX.LOCAL

Health Check:

Corrective Actions: Make sure Netlogon content has no malicious extensions or unnecessary content.

Account Security Assessment

The following section provide a summary of the Account Security Assessment on Domain PHARMAX.LOCAL.



Total Users	2889
Enabled Users	2885
Disabled Users	4
Enabled Inactive Users	1
Users With Reversible Encryption Password	3
Password Not Required	4
Password Never Expires	19
Kerberos DES Users	1

Does Not Require Pre Auth	0
Users With SID History	0

Table 22 - Account Security Assessment - PHARMAX.LOCAL

Health Check:

Corrective Actions: *Ensure there aren't any account with weak security posture.*

Unconstrained Kerberos Delegation

The following section provide a summary of unconstrained kerberos delegation on Domain PHARMAX.LOCAL.

Name	Distinguished Name
HV-SERVER-01V	CN=HV-SERVER-01V,OU=Member Servers,DC=pharmax,DC=local

Table 23 - Unconstrained Kerberos Delegation - PHARMAX.LOCAL

Health Check:

Corrective Actions: *Ensure there aren't any unconstrained kerberos delegation in Active Directory.*

KRBTGT Account Audit

The following section provide a summary of KRBTGT account on Domain PHARMAX.LOCAL.

Name	krbtgt
Created	06/10/2018 21:00:49
Password Last Set	06/10/2018 21:00:49
Distinguished Name	CN=krbtgt,CN=Users,DC=pharmax,DC=local

Table 24 - KRBTGT Account Audit - PHARMAX.LOCAL

Health Check:

Best Practice: *Microsoft advises changing the krbtgt account password at regular intervals to keep the environment more secure.*

Administrator Account Audit

The following section provide a summary of Administrator account on Domain PHARMAX.LOCAL.

Name	Administrator
Created	06/10/2018 21:00:05
Password Last Set	06/10/2018 04:01:50
Last Logon Date	12/10/2053 19:01:07
Distinguished Name	CN=Administrator,CN=Users,DC=pharmax,DC=local

Table 25 - Administrator Account Audit - PHARMAX.LOCAL

Health Check:

Best Practice: Microsoft advises changing the administrator account password at regular intervals to keep the environment more secure.

Duplicate Objects

The following section details Duplicate Objects discovered on Domain PHARMAX.LOCAL.

Name	Created	Changed	Conflict Changed
SCCM-DP-01V-Remote-Installation-Services CNF:0b206bf4-6c39-47b2-bd69-3694aa657d76	2020:09:13	2020:09:13	2020:09:13

Table 26 - Duplicate Object - PHARMAX.LOCAL

Health Check:

Corrective Actions: Ensure there aren't any duplicate object.

1.2.1.14 Domain Controller Summary

A domain controller (DC) is a server computer that responds to security authentication requests within a computer network domain. It is a network server that is responsible for allowing host access to domain resources. It authenticates users, stores user account information and enforces security policy for a domain.

DC Name	Domain Name	Site	Global Catalog	Read Only	IP Address
SERVER-DC-01V	pharmax.local	Pharmax-HQ	Yes	No	192.168.5.1

Table 27 - Domain Controller Summary - PHARMAX.LOCAL

1.2.1.14.1 Hardware Inventory

The following section provides detailed Domain Controller Hardware information for domain PHARMAX.LOCAL.

Name	Number of Processors	Number of CPU Cores	Physical Memory
SERVER-DC-01V	1	2	4.00 GB
CAYEY-DC-01V	1	2	4.00 GB

Table 28 - Hardware Inventory - PHARMAX.LOCAL

1.2.1.14.2 NTDS Information

DC Name	Database File	Database Size	Log Path	SysVol Path
CAYEY-DC-01V	C:\Windows\NTDS\ntds.dit	72.00 MB	C:\Windows\NTDS	C:\Windows\SYSVOL\sysvol
SERVER-DC-01V	C:\Windows\NTDS\ntds.dit	80.00 MB	C:\Windows\NTDS	C:\Windows\SYSVOL\sysvol

Table 29 - NTDS Database File Usage - PHARMAX.LOCAL

1.2.1.14.3 Time Source Information

Name	Time Server	Type
CAYEY-DC-01V	Domain Hierarchy	DOMHIER
SERVER-DC-01V	192.168.5.254 0.pool.ntp.org 1.pool.ntp.org 2.pool.ntp.org 3.pool.ntp.org	MANUAL (NTP)

Table 30 - Time Source Configuration - PHARMAX.LOCAL

1.2.1.14.4 SRV Records Status

Name	A Record	KDC SRV	PDC SRV	GC SRV	DC SRV
SERVER-DC-01V	OK	OK	OK	OK	OK

Table 31 - SRV Records Status - PHARMAX.LOCAL

Health Check:

Best Practice: The SRV record is a Domain Name System (DNS) resource record. It's used to identify computers hosting specific services. SRV resource records are used to locate domain controllers for Active Directory.

1.2.1.14.5 Installed Software

The following section provides a summary of additional software running on Domain Controllers from domain PHARMAX.LOCAL.

SERVER-DC-01V

Name	Publisher	Install Date
7-Zip 19.00 (x64)	Igor Pavlov	-
DiskMax 6.21	KoshyJohn.com	17/11/2021
Google Chrome	Google LLC	20230313
Npcap	Nmap Project	-
RVTools	Robware	20220824

Microsoft Active Directory As Built Report - v1.0

Name	Publisher	Install Date
Veeam Agent for Microsoft Windows	Veeam Software Group GmbH	20230215
Veeam Backup Transport	Veeam Software Group GmbH	20230215
Veeam Backup VSS Integration	Veeam Software Group GmbH	20230215
Veeam Installer Service	Veeam Software Group GmbH	-
Veeam VSS Hardware Provider	Veeam Software Group GmbH	20230216

Table 32 - Installed Software - SERVER-DC-01V

Health Check:

Best Practices: Do not run other software or services on a Domain Controller.

CAYEY-DC-01V

Name	Publisher	Install Date
7-Zip 21.07 (x64 edition)	Igor Pavlov	20220122

Table 33 - Installed Software - CAYEY-DC-01V

Health Check:

Best Practices: Do not run other software or services on a Domain Controller.

1.2.1.14.6 DC Diagnostic

The following section provides a summary of the Active Directory DC Diagnostic.

SERVER-DC-01V

Test Name	Result	Impact	Description
Replications	Failed	High	Makes a deep validation to check the main replication for all naming contexts in this Domain Controller.
RidManager	Passed	High	Validates this Domain Controller can locate and contact the RID Master FSMO role holder. This test is skipped in RODCs.
ObjectsReplicated	Passed	High	Checks the replication health of core objects and attributes.
NCSecDesc	Passed	Medium	Validates if permissions are correctly set in this Domain Controller for all naming contexts. Those permissions directly affect replications health.
NetLogons	Passed	High	Validates if core security groups (including administrators and Authenticated Users) can connect and read NETLOGON and SYSVOL folders. It also validates access to IPC\$. which can lead to failures in organizations that disable IPC\$.
Services	Passed	High	Validates if the core Active Directory services are running in this Domain Controller. The services verified are: RPCSS, EVENTSYSTEM, DNSCACHE, ISMSERV, KDC,

Microsoft Active Directory As Built Report - v1.0

Test Name	Result	Impact	Description
			SAMSS, WORKSTATION, W32TIME, NETLOGON, NTDS (in case Windows Server 2008 or newer) and DFSR (if SYSVOL is using DFSR).
VerifyReplicas	Passed	High	Checks that all application directory partitions are fully instantiated on all replica servers.
DNS	Passed	Medium	DNS Includes six optional DNS-related tests, as well as the Connectivity test, which runs by default.
VerifyReferences	Passed	High	Validates that several attributes are present for the domain in the container and subcontainers in the DC objects. This test will fail if any attribute is missing.
SystemLog	Failed	Low	Checks if there is any errors in the Event Viewer > System event log in the past 60 minutes. Since the System event log records data from many places, errors reported here may lead to false positive and must be investigated further. The impact of this validation is marked as Low.
Topology	Passed	Medium	Topology Checks that the KCC has generated a fully connected topology for all domain controllers.
CutoffServers	Passed	Medium	Checks for any server that is not receiving replications because its partners are not running
FrsEvent	Passed	Medium	Checks if theres any errors in the event logs regarding FRS replication. If running Windows Server 2008 R2 or newer on all Domain Controllers is possible SYSVOL were already migrated to DFSR, in this case errors found here can be ignored.
CheckSecurityError	Passed	Medium	Reports on the overall health of replication with respect to Active Directory security in domain controllers running Windows Server 2003 SP1.
Connectivity	Passed	Medium	Initial connection validation, checks if the DC can be located in the DNS, validates the ICMP ping (1 hop), checks LDAP binding and also the RPC connection. This initial test requires ICMP, LDAP, DNS and RPC connectivity to work properly.
Advertising	Passed	High	Validates this Domain Controller can be correctly located through the KDC service. It does not validate the Kerberos tickets answer or the communication through the TCP and UDP port 88.
DFSREvent	Failed	Medium	Checks if theres any errors in the event logs regarding DFSR replication. If running Windows Server 2008 or older on all Domain Controllers is possible SYSVOL is still using FRS, and in this case errors found here can be ignored. Obs. is highly recommended to migrate SYSVOL to DFSR.
KnowsOfRoleHolders	Passed	High	Checks if this Domain Controller is aware of which DC (or DCs) hold the FSMOs.

Microsoft Active Directory As Built Report - v1.0

Test Name	Result	Impact	Description
MachineAccount	Passed	High	Checks if this computer account exist in Active Directory and the main attributes are set. If this validation reports error. the following parameters of DCDIAG might help: /RecreateMachineAccount and /FixMachineAccount.
KccEvent	Failed	High	Validates through KCC there were no errors in the Event Viewer > Applications and Services Logs > Directory Services event log in the past 15 minutes (default time).
SysVolCheck	Passed	High	Validates if the registry key HKEY_Local_Machine\System\CurrentControlSet\Services\Netlogon\Parameters\SysvolReady=1 exist. This registry has to exist with value 1 for the DCs SYSVOL to be advertised.
FrsSysVol	Passed	Medium	Checks that the file replication system (FRS) system volume (SYSVOL) is ready

Table 34 - DCDiag Test Status - SERVER-DC-01V

CAYEY-DC-01V

Test Name	Result	Impact	Description
Replications	Failed	High	Makes a deep validation to check the main replication for all naming contexts in this Domain Controller.
RidManager	Passed	High	Validates this Domain Controller can locate and contact the RID Master FSMO role holder. This test is skipped in RODCs.
ObjectsReplicated	Passed	High	Checks the replication health of core objects and attributes.
NCSecDesc	Passed	Medium	Validates if permissions are correctly set in this Domain Controller for all naming contexts. Those permissions directly affect replications health.
NetLogons	Passed	High	Validates if core security groups (including administrators and Authenticated Users) can connect and read NETLOGON and SYSVOL folders. It also validates access to IPC\$. which can lead to failures in organizations that disable IPC\$.
Services	Passed	High	Validates if the core Active Directory services are running in this Domain Controller. The services verified are: RPCSS, EVENTSYSTEM, DNSCACHE, ISMSERV, KDC, SAMSS, WORKSTATION, W32TIME, NETLOGON, NTDS (in case Windows Server 2008 or newer) and DFSR (if SYSVOL is using DFSR).
VerifyReplicas	Passed	High	Checks that all application directory partitions are fully instantiated on all replica servers.
DNS	Failed	Medium	DNS Includes six optional DNS-related tests, as well as the Connectivity test, which runs by default.

Microsoft Active Directory As Built Report - v1.0

Test Name	Result	Impact	Description
VerifyReferences	Passed	High	Validates that several attributes are present for the domain in the container and subcontainers in the DC objects. This test will fail if any attribute is missing.
SystemLog	Failed	Low	Checks if there is any errors in the Event Viewer > System event log in the past 60 minutes. Since the System event log records data from many places, errors reported here may lead to false positive and must be investigated further. The impact of this validation is marked as Low.
Topology	Passed	Medium	Topology Checks that the KCC has generated a fully connected topology for all domain controllers.
CutoffServers	Passed	Medium	Checks for any server that is not receiving replications because its partners are not running
FrsEvent	Passed	Medium	Checks if there are any errors in the event logs regarding FRS replication. If running Windows Server 2008 R2 or newer on all Domain Controllers is possible SYSVOL were already migrated to DFSR, in this case errors found here can be ignored.
CheckSecurityError	Passed	Medium	Reports on the overall health of replication with respect to Active Directory security in domain controllers running Windows Server 2003 SP1.
Connectivity	Passed	Medium	Initial connection validation, checks if the DC can be located in the DNS, validates the ICMP ping (1 hop), checks LDAP binding and also the RPC connection. This initial test requires ICMP, LDAP, DNS and RPC connectivity to work properly.
Advertising	Passed	High	Validates this Domain Controller can be correctly located through the KDC service. It does not validate the Kerberos tickets answer or the communication through the TCP and UDP port 88.
DFSREvent	Failed	Medium	Checks if there are any errors in the event logs regarding DFSR replication. If running Windows Server 2008 or older on all Domain Controllers is possible SYSVOL is still using FRS, and in this case errors found here can be ignored. Obs. is highly recommended to migrate SYSVOL to DFSR.
KnowsOfRoleHolders	Passed	High	Checks if this Domain Controller is aware of which DC (or DCs) hold the FSMOs.
MachineAccount	Passed	High	Checks if this computer account exist in Active Directory and the main attributes are set. If this validation reports error. the following parameters of DCDIAG might help: /RecreateMachineAccount and /FixMachineAccount.
KccEvent	Failed	High	Validates through KCC there were no errors in the Event Viewer > Applications and Services Logs > Directory Services event log in the past 15 minutes (default time).

Microsoft Active Directory As Built Report - v1.0

Test Name	Result	Impact	Description
SysVolCheck	Passed	High	Validates if the registry key HKEY_Local_Machine\System\CurrentControlSet\Services\Netlogon\Parameters\SysvolReady=1 exist. This registry has to exist with value 1 for the DCs SYSVOL to be advertised.
FrsSysVol	Passed	Medium	Checks that the file replication system (FRS) system volume (SYSVOL) is ready

Table 35 - DCDiag Test Status - CAYEY-DC-01V

1.2.1.14.7 Infrastructure Services Status

The following section provides a summary of the Domain Controller Infrastructure services status.

SERVER-DC-01V

Display Name	Short Name	Status
Active Directory Certificate Services	CertSvc	Running
Active Directory Domain Services	NTDS	Running
Active Directory Web Services	ADWS	Running
COM+ Event System	EVENTSYSTEM	Running
DFS Replication	DFSR	Running
DHCP Server	DHCPServer	Running
DNS Client	DNSCACHE	Running
DNS Server	DNS	Running
Intersite Messaging	Ismserv	Running
Kerberos Key Distribution Center	Kdc	Running
NetLogon	Netlogon	Running
Print Spooler	Spooler	Running
Remote Procedure Call (RPC)	RPCSS	Running
Security Accounts Manager	SAMSS	Running
Windows Time	W32Time	Running
WORKSTATION	LanmanWorkstation	Running

Table 36 - Infrastructure Services Status - SERVER-DC-01V

Health Check:

Corrective Actions: Disable Print Spooler service on DCs and all servers that do not perform Print services.

CAYEY-DC-01V

Display Name	Short Name	Status
Active Directory Certificate Services	CertSvc	Running
Active Directory Domain Services	NTDS	Running

Microsoft Active Directory As Built Report - v1.0

Display Name	Short Name	Status
Active Directory Web Services	ADWS	Running
COM+ Event System	EVENTSYSTEM	Running
DFS Replication	DFSR	Running
DHCP Server	DHCPServer	Running
DNS Client	DNSCACHE	Running
DNS Server	DNS	Running
Intersite Messaging	IsmServ	Running
Kerberos Key Distribution Center	Kdc	Running
NetLogon	Netlogon	Running
Print Spooler	Spooler	Running
Remote Procedure Call (RPC)	RPCSS	Running
Security Accounts Manager	SAMSS	Running
Windows Time	W32Time	Running
WORKSTATION	LanmanWorkstation	Running

Table 37 - Infrastructure Services Status - CAYEY-DC-01V

Health Check:

Corrective Actions: Disable Print Spooler service on DCs and all servers that do not perform Print services.

1.2.1.14.8 Sites Replication Connection

The following section provide summary information about Site Replication Connection.

Replicate From Directory Server	Replicate To Directory Server	Transport Protocol	Auto Generated	Enabled
ACADE-DC-01V	SERVER-DC-01V	IP	Yes	Yes
CAYEY-DC-01V	SERVER-DC-01V	IP	Yes	Yes
DC-UIA-01V	SERVER-DC-01V	IP	Yes	Yes

Table 38 - Site Replication - PHARMAX.LOCAL

1.2.1.14.9 Sites Replication Status

Source DSA	Destination DSA	Source DSA Site	Last Success Time	Last Failure Status	Last Failure Time	Number of failures
ACADE-DC-01V	SERVER-DC-01V	ACAD	2023-03-14 09:23:56	0	0	0
ACADE-DC-01V	SERVER-DC-01V	ACAD	2023-03-14 09:23:56	0	0	0
ACADE-DC-01V	SERVER-DC-01V	ACAD	2023-03-14 09:24:03	0	0	0

Microsoft Active Directory As Built Report - v1.0

Source DSA	Destination DSA	Source DSA Site	Last Success Time	Last Failure Status	Last Failure Time	Number of failures
ACADE-DC-01V	SERVER-DC-01V	ACAD	2023-03-14 09:24:03	0	0	0
ACADE-DC-01V	SERVER-DC-01V	ACAD	2023-03-14 09:24:03	0	0	0
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2023-03-14 09:24:03	0	0	0
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2023-03-14 09:24:03	0	0	0
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2023-03-14 09:23:49	0	0	0
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2023-03-14 09:23:49	0	0	0
CAYEY-DC-01V	SERVER-DC-01V	Cayey-Branch	2023-03-14 09:23:56	0	0	0
DC-UIA-01V	SERVER-DC-01V	UIA	2023-03-10 22:48:44	1256	2023-03-14 09:23:56	154
DC-UIA-01V	SERVER-DC-01V	UIA	2023-03-10 22:48:44	1256	2023-03-14 09:23:56	149
DC-UIA-01V	SERVER-DC-01V	UIA	2023-03-10 22:48:44	8524	2023-03-14 09:24:03	154
DC-UIA-01V	SERVER-DC-01V	UIA	2023-03-10 22:48:44	8524	2023-03-14 09:23:56	154
DC-UIA-01V	SERVER-DC-01V	UIA	2023-03-10 22:48:44	1256	2023-03-14 09:23:56	149

Table 39 - Site Replication Status - PHARMAX.LOCAL

Health Check:

Best Practices: Replication failure can lead to object inconsistencies and major problems in Active Directory.

1.2.1.14.10 Group Policy Objects Summary

The following section provides a summary of the Group Policy Objects for domain PHARMAX.LOCAL.

GPO Name	GPO Status	Owner
Assign-Applications	All Settings Enabled	PHARMAX\Domain Admins
Certificate AutoEnrollment	User Settings Disabled	PHARMAX\Domain Admins
Dead Policy	All Settings Disabled	PHARMAX\Domain Admins
Default Domain Controllers Policy	All Settings Enabled	PHARMAX\Domain Admins
Default Domain Policy	All Settings Enabled	PHARMAX\Domain Admins
Horizon-DEM	All Settings Enabled	PHARMAX\Domain Admins

Microsoft Active Directory As Built Report - v1.0

GPO Name	GPO Status	Owner
LAPS Configuration	All Settings Enabled	PHARMAX\Domain Admins
Linux-Settings-GPO	All Settings Disabled	PHARMAX\Domain Admins
ProfileUnity	All Settings Enabled	PHARMAX\Domain Admins
SCCM - Restricted Group and General Settings	All Settings Enabled	PHARMAX\Domain Admins
SCEP Configuration	All Settings Enabled	PHARMAX\Domain Admins
SET - KMS Server	All Settings Enabled	PHARMAX\Domain Admins
VEEAM_Disable_Firewall	All Settings Enabled	PHARMAX\Domain Admins
VEEAM_Local_Administrators	All Settings Enabled	PHARMAX\Domain Admins
WSUS - Domain Policy	User Settings Disabled	PHARMAX\Domain Admins

Table 40 - GPO - PHARMAX.LOCAL

Health Check:

Best Practices: Ensure 'All Settings Disabled' GPO are removed from Active Directory.

1.2.1.14.10.1 Central Store Repository

Domain	Configured	Central Store Path
PHARMAX.LOCAL	Yes	\\pharmax.local\SYSVOL\pharmax.local\Policies\PolicyDefinitions

Table 41 - GPO Central Store - PHARMAX.LOCAL

1.2.1.14.10.2 User Logon/Logoff Script

GPO Name	GPO Status	Type	Script
Dead Policy	All Settings Disabled	Logoff	%systemdrive%\Program Files\ProfileUnity\Client.NET\LwL.ProfileUnity.Client.Logoff.exe
Horizon-DEM	All Settings Enabled	Logoff	C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe
ProfileUnity	All Settings Enabled	Logoff	%systemdrive%\Program Files\ProfileUnity\Client.NET\LwL.ProfileUnity.Client.Logoff.exe

Table 42 - GPO with Logon/Logoff Script - PHARMAX.LOCAL

1.2.1.14.10.3 Computer Startup/Shutdown Script

GPO Name	GPO Status	Type	Script
Dead Policy	All Settings Disabled	Startup	\\pharmax.local\netlogon\profileunity\LwL.ProfileUnity.Client.Startup.exe

Microsoft Active Directory As Built Report - v1.0

GPO Name	GPO Status	Type	Script
ProfileUnity	All Settings Enabled	Startup	\\pharmax.local\netlogon\profileunity\LwL.Profile Unity.Client.Startup.exe

Table 43 - GPO with Startup/Shutdown Script - PHARMAX.LOCAL

1.2.1.14.10.4 Unlinked GPO

GPO Name	Created	Modified	Computer Enabled	User Enabled
Assign-Applications	2021-03-11	2021-03-11	Yes	Yes
Dead Policy	2021-10-05	2022-01-22	No	No

Table 44 - Unlinked GPO - PHARMAX.LOCAL

Health Check:

Corrective Actions: Remove Unused GPO from Active Directory.

1.2.1.14.10.5 Empty GPOs

GPO Name	Created	Modified	Description
Linux-Settings-GPO	2021-05-23	2022-02-04	-

Table 45 - Empty GPO - PHARMAX.LOCAL

Health Check:

Corrective Actions: No User and Computer parameters are set: Remove Unused GPO in Active Directory.

1.2.1.14.10.6 Enforced GPO

GPO Name	Enforced	Order	Target
Linux-Settings-GPO	Yes	1	pharmax.local/LinuxMachines

Table 46 - Enforced GPO - PHARMAX.LOCAL

Health Check:

Corrective Actions: Review use of enforcement and blocked policy inheritance in Active Directory.

1.2.1.14.11 Organizational Units

The following section provides a summary of Active Directory Organizational Unit information.

Name	Path	Linked GPO
.SecFrame.com	pharmax.local/.SecFrame.com	-

Microsoft Active Directory As Built Report - v1.0

Name	Path	Linked GPO
Admin	pharmax.local/Admin	-
Staging	pharmax.local/Admin/Staging	-
Tier 0	pharmax.local/Admin/Tier 0	-
T0-Accounts	pharmax.local/Admin/Tier 0/T0-Accounts	-
T0-Devices	pharmax.local/Admin/Tier 0/T0-Devices	-
T0-Permissions	pharmax.local/Admin/Tier 0/T0-Permissions	-
T0-Roles	pharmax.local/Admin/Tier 0/T0-Roles	-
T0-Servers	pharmax.local/Admin/Tier 0/T0-Servers	-
Tier 1	pharmax.local/Admin/Tier 1	-
T1-Accounts	pharmax.local/Admin/Tier 1/T1-Accounts	-
T1-Devices	pharmax.local/Admin/Tier 1/T1-Devices	-
T1-Permissions	pharmax.local/Admin/Tier 1/T1-Permissions	-
T1-Roles	pharmax.local/Admin/Tier 1/T1-Roles	-
T1-Servers	pharmax.local/Admin/Tier 1/T1-Servers	-
Tier 2	pharmax.local/Admin/Tier 2	-
T2-Accounts	pharmax.local/Admin/Tier 2/T2-Accounts	-
T2-Devices	pharmax.local/Admin/Tier 2/T2-Devices	-
T2-Permissions	pharmax.local/Admin/Tier 2/T2-Permissions	-
T2-Roles	pharmax.local/Admin/Tier 2/T2-Roles	-
T2-Servers	pharmax.local/Admin/Tier 2/T2-Servers	-
Admins PC	pharmax.local/Admins PC	-
Configuration Manager	pharmax.local/Configuration Manager	SCEP Configuration, SCCM - Restricted Group and General Settings
Configuration Manager Computers	pharmax.local/Configuration Manager Computers	LAPS Configuration, SCEP Configuration
Domain Controllers	pharmax.local/Domain Controllers	Default Domain Controllers Policy
EMC NAS servers	pharmax.local/EMC NAS servers	-
Computers	pharmax.local/EMC NAS servers/Computers	-
Fortinet EMS	pharmax.local/Fortinet EMS	-
Grouper-Groups	pharmax.local/Grouper-Groups	-
LinuxMachines	pharmax.local/LinuxMachines	Linux-Settings-GPO
Member Servers	pharmax.local/Member Servers	-
People	pharmax.local/People	-
AWS	pharmax.local/People/AWS	-

Microsoft Active Directory As Built Report - v1.0

Name	Path	Linked GPO
AZR	pharmax.local/People/AZR	-
BDE	pharmax.local/People/BDE	-
Deprovisioned	pharmax.local/People/Deprovisioned	-
ESM	pharmax.local/People/ESM	-
FIN	pharmax.local/People/FIN	-
FSR	pharmax.local/People/FSR	-
GOO	pharmax.local/People/GOO	-
HRE	pharmax.local/People/HRE	-
ITS	pharmax.local/People/ITS	-
OGC	pharmax.local/People/OGC	-
SEC	pharmax.local/People/SEC	-
TST	pharmax.local/People/TST	-
Unassociated	pharmax.local/People/Unassociated	-
ProfileUnity VDI	pharmax.local/ProfileUnity VDI	VEEAM_Local_Administrators, VEEAM_Disable_Firewall
Computers	pharmax.local/ProfileUnity VDI/Computers	ProfileUnity
Servers	pharmax.local/ProfileUnity VDI/Servers	-
Quarantine	pharmax.local/Quarantine	-
Stage	pharmax.local/Stage	-
AWS	pharmax.local/Stage/AWS	-
Devices	pharmax.local/Stage/AWS/Devices	-
Groups	pharmax.local/Stage/AWS/Groups	-
ServiceAccounts	pharmax.local/Stage/AWS/ServiceAccounts	-
Test	pharmax.local/Stage/AWS/Test	-
AZR	pharmax.local/Stage/AZR	-
Devices	pharmax.local/Stage/AZR/Devices	-
Groups	pharmax.local/Stage/AZR/Groups	-
ServiceAccounts	pharmax.local/Stage/AZR/ServiceAccounts	-
Test	pharmax.local/Stage/AZR/Test	-
BDE	pharmax.local/Stage/BDE	-
Devices	pharmax.local/Stage/BDE/Devices	-
Groups	pharmax.local/Stage/BDE/Groups	-
ServiceAccounts	pharmax.local/Stage/BDE/ServiceAccounts	-
Test	pharmax.local/Stage/BDE/Test	-
ESM	pharmax.local/Stage/ESM	-
Devices	pharmax.local/Stage/ESM/Devices	-
Groups	pharmax.local/Stage/ESM/Groups	-

Microsoft Active Directory As Built Report - v1.0

Name	Path	Linked GPO
ServiceAccounts	pharmax.local/Stage/ESM/ServiceAccounts	-
Test	pharmax.local/Stage/ESM/Test	-
FIN	pharmax.local/Stage/FIN	-
Devices	pharmax.local/Stage/FIN/Devices	-
Groups	pharmax.local/Stage/FIN/Groups	-
ServiceAccounts	pharmax.local/Stage/FIN/ServiceAccounts	-
Test	pharmax.local/Stage/FIN/Test	-
FSR	pharmax.local/Stage/FSR	-
Devices	pharmax.local/Stage/FSR/Devices	-
Groups	pharmax.local/Stage/FSR/Groups	-
ServiceAccounts	pharmax.local/Stage/FSR/ServiceAccounts	-
Test	pharmax.local/Stage/FSR/Test	-
GOO	pharmax.local/Stage/GOO	-
Devices	pharmax.local/Stage/GOO/Devices	-
Groups	pharmax.local/Stage/GOO/Groups	-
ServiceAccounts	pharmax.local/Stage/GOO/ServiceAccounts	-
Test	pharmax.local/Stage/GOO/Test	-
HRE	pharmax.local/Stage/HRE	-
Devices	pharmax.local/Stage/HRE/Devices	-
Groups	pharmax.local/Stage/HRE/Groups	-
ServiceAccounts	pharmax.local/Stage/HRE/ServiceAccounts	-
Test	pharmax.local/Stage/HRE/Test	-
ITS	pharmax.local/Stage/ITS	-
Devices	pharmax.local/Stage/ITS/Devices	-
Groups	pharmax.local/Stage/ITS/Groups	-
ServiceAccounts	pharmax.local/Stage/ITS/ServiceAccounts	-
Test	pharmax.local/Stage/ITS/Test	-
OGC	pharmax.local/Stage/OGC	-
Devices	pharmax.local/Stage/OGC/Devices	-
Groups	pharmax.local/Stage/OGC/Groups	-
ServiceAccounts	pharmax.local/Stage/OGC/ServiceAccounts	-
Test	pharmax.local/Stage/OGC/Test	-
SEC	pharmax.local/Stage/SEC	-
Devices	pharmax.local/Stage/SEC/Devices	-

Microsoft Active Directory As Built Report - v1.0

Name	Path	Linked GPO
Groups	pharmax.local/Stage/SEC/Groups	-
ServiceAccounts	pharmax.local/Stage/SEC/ServiceAccounts	-
Test	pharmax.local/Stage/SEC/Test	-
TST	pharmax.local/Stage/TST	-
Devices	pharmax.local/Stage/TST/Devices	-
Groups	pharmax.local/Stage/TST/Groups	-
ServiceAccounts	pharmax.local/Stage/TST/ServiceAccounts	-
Test	pharmax.local/Stage/TST/Test	-
Testing	pharmax.local/Testing	-
Tier 1	pharmax.local/Tier 1	-
AWS	pharmax.local/Tier 1/AWS	-
Devices	pharmax.local/Tier 1/AWS/Devices	-
Groups	pharmax.local/Tier 1/AWS/Groups	-
ServiceAccounts	pharmax.local/Tier 1/AWS/ServiceAccounts	-
Test	pharmax.local/Tier 1/AWS/Test	-
AZR	pharmax.local/Tier 1/AZR	-
Devices	pharmax.local/Tier 1/AZR/Devices	-
Groups	pharmax.local/Tier 1/AZR/Groups	-
ServiceAccounts	pharmax.local/Tier 1/AZR/ServiceAccounts	-
Test	pharmax.local/Tier 1/AZR/Test	-
BDE	pharmax.local/Tier 1/BDE	-
Devices	pharmax.local/Tier 1/BDE/Devices	-
Groups	pharmax.local/Tier 1/BDE/Groups	-
ServiceAccounts	pharmax.local/Tier 1/BDE/ServiceAccounts	-
Test	pharmax.local/Tier 1/BDE/Test	-
ESM	pharmax.local/Tier 1/ESM	-
Devices	pharmax.local/Tier 1/ESM/Devices	-
Groups	pharmax.local/Tier 1/ESM/Groups	-
ServiceAccounts	pharmax.local/Tier 1/ESM/ServiceAccounts	-
Test	pharmax.local/Tier 1/ESM/Test	-
FIN	pharmax.local/Tier 1/FIN	-
Devices	pharmax.local/Tier 1/FIN/Devices	-
Groups	pharmax.local/Tier 1/FIN/Groups	-
ServiceAccounts	pharmax.local/Tier 1/FIN/ServiceAccounts	-

Microsoft Active Directory As Built Report - v1.0

Name	Path	Linked GPO
Test	pharmax.local/Tier 1/FIN/Test	-
FSR	pharmax.local/Tier 1/FSR	-
Devices	pharmax.local/Tier 1/FSR/Devices	-
Groups	pharmax.local/Tier 1/FSR/Groups	-
ServiceAccounts	pharmax.local/Tier 1/FSR/ServiceAccounts	-
Test	pharmax.local/Tier 1/FSR/Test	-
GOO	pharmax.local/Tier 1/GOO	-
Devices	pharmax.local/Tier 1/GOO/Devices	-
Groups	pharmax.local/Tier 1/GOO/Groups	-
ServiceAccounts	pharmax.local/Tier 1/GOO/ServiceAccounts	-
Test	pharmax.local/Tier 1/GOO/Test	-
HRE	pharmax.local/Tier 1/HRE	-
Devices	pharmax.local/Tier 1/HRE/Devices	-
Groups	pharmax.local/Tier 1/HRE/Groups	-
ServiceAccounts	pharmax.local/Tier 1/HRE/ServiceAccounts	-
Test	pharmax.local/Tier 1/HRE/Test	-
ITS	pharmax.local/Tier 1/ITS	-
Devices	pharmax.local/Tier 1/ITS/Devices	-
Groups	pharmax.local/Tier 1/ITS/Groups	-
ServiceAccounts	pharmax.local/Tier 1/ITS/ServiceAccounts	-
Test	pharmax.local/Tier 1/ITS/Test	-
OGC	pharmax.local/Tier 1/OGC	-
Devices	pharmax.local/Tier 1/OGC/Devices	-
Groups	pharmax.local/Tier 1/OGC/Groups	-
ServiceAccounts	pharmax.local/Tier 1/OGC/ServiceAccounts	-
Test	pharmax.local/Tier 1/OGC/Test	-
SEC	pharmax.local/Tier 1/SEC	-
Devices	pharmax.local/Tier 1/SEC/Devices	-
Groups	pharmax.local/Tier 1/SEC/Groups	-
ServiceAccounts	pharmax.local/Tier 1/SEC/ServiceAccounts	-
Test	pharmax.local/Tier 1/SEC/Test	-
TST	pharmax.local/Tier 1/TST	-
Devices	pharmax.local/Tier 1/TST/Devices	-
Groups	pharmax.local/Tier 1/TST/Groups	-

Microsoft Active Directory As Built Report - v1.0

Name	Path	Linked GPO
ServiceAccounts	pharmax.local/Tier 1/TST/ServiceAccounts	-
Test	pharmax.local/Tier 1/TST/Test	-
Tier 2	pharmax.local/Tier 2	-
AWS	pharmax.local/Tier 2/AWS	-
Devices	pharmax.local/Tier 2/AWS/Devices	-
Groups	pharmax.local/Tier 2/AWS/Groups	-
ServiceAccounts	pharmax.local/Tier 2/AWS/ServiceAccounts	-
Test	pharmax.local/Tier 2/AWS/Test	-
AZR	pharmax.local/Tier 2/AZR	-
Devices	pharmax.local/Tier 2/AZR/Devices	-
Groups	pharmax.local/Tier 2/AZR/Groups	-
ServiceAccounts	pharmax.local/Tier 2/AZR/ServiceAccounts	-
Test	pharmax.local/Tier 2/AZR/Test	-
BDE	pharmax.local/Tier 2/BDE	-
Devices	pharmax.local/Tier 2/BDE/Devices	-
Groups	pharmax.local/Tier 2/BDE/Groups	-
ServiceAccounts	pharmax.local/Tier 2/BDE/ServiceAccounts	-
Test	pharmax.local/Tier 2/BDE/Test	-
ESM	pharmax.local/Tier 2/ESM	-
Devices	pharmax.local/Tier 2/ESM/Devices	-
Groups	pharmax.local/Tier 2/ESM/Groups	-
ServiceAccounts	pharmax.local/Tier 2/ESM/ServiceAccounts	-
Test	pharmax.local/Tier 2/ESM/Test	-
FIN	pharmax.local/Tier 2/FIN	-
Devices	pharmax.local/Tier 2/FIN/Devices	-
Groups	pharmax.local/Tier 2/FIN/Groups	-
ServiceAccounts	pharmax.local/Tier 2/FIN/ServiceAccounts	-
Test	pharmax.local/Tier 2/FIN/Test	-
FSR	pharmax.local/Tier 2/FSR	-
Devices	pharmax.local/Tier 2/FSR/Devices	-
Groups	pharmax.local/Tier 2/FSR/Groups	-
ServiceAccounts	pharmax.local/Tier 2/FSR/ServiceAccounts	-
Test	pharmax.local/Tier 2/FSR/Test	-
GOO	pharmax.local/Tier 2/GOO	-

Microsoft Active Directory As Built Report - v1.0

Name	Path	Linked GPO
Devices	pharmax.local/Tier 2/GOO/Devices	-
Groups	pharmax.local/Tier 2/GOO/Groups	-
ServiceAccounts	pharmax.local/Tier 2/GOO/ServiceAccounts	-
Test	pharmax.local/Tier 2/GOO/Test	-
HRE	pharmax.local/Tier 2/HRE	-
Devices	pharmax.local/Tier 2/HRE/Devices	-
Groups	pharmax.local/Tier 2/HRE/Groups	-
ServiceAccounts	pharmax.local/Tier 2/HRE/ServiceAccounts	-
Test	pharmax.local/Tier 2/HRE/Test	-
ITS	pharmax.local/Tier 2/ITS	-
Devices	pharmax.local/Tier 2/ITS/Devices	-
Groups	pharmax.local/Tier 2/ITS/Groups	-
ServiceAccounts	pharmax.local/Tier 2/ITS/ServiceAccounts	-
Test	pharmax.local/Tier 2/ITS/Test	-
OGC	pharmax.local/Tier 2/OGC	-
Devices	pharmax.local/Tier 2/OGC/Devices	-
Groups	pharmax.local/Tier 2/OGC/Groups	-
ServiceAccounts	pharmax.local/Tier 2/OGC/ServiceAccounts	-
Test	pharmax.local/Tier 2/OGC/Test	-
SEC	pharmax.local/Tier 2/SEC	-
Devices	pharmax.local/Tier 2/SEC/Devices	-
Groups	pharmax.local/Tier 2/SEC/Groups	-
ServiceAccounts	pharmax.local/Tier 2/SEC/ServiceAccounts	-
Test	pharmax.local/Tier 2/SEC/Test	-
TST	pharmax.local/Tier 2/TST	-
Devices	pharmax.local/Tier 2/TST/Devices	-
Groups	pharmax.local/Tier 2/TST/Groups	-
ServiceAccounts	pharmax.local/Tier 2/TST/ServiceAccounts	-
Test	pharmax.local/Tier 2/TST/Test	-
VDI-Computers	pharmax.local/VDI-Computers	Horizon-DEM
Finances	pharmax.local/VDI-Computers/Finances	-
HR	pharmax.local/VDI-Computers/HR	-
Marketing	pharmax.local/VDI-Computers/Marketing	-
Sales	pharmax.local/VDI-Computers/Sales	-

Name	Path	Linked GPO
VEEAM Servers	pharmax.local/VEEAM Servers	VEEAM_Disable_Firewall, VEEAM_Local_Administrators
VEEAM WorkStations	pharmax.local/VEEAM WorkStations	VEEAM_Local_Administrators, VEEAM_Disable_Firewall

Table 47 - Organizational Unit - PHARMAX.LOCAL

1.2.1.14.11.1 GPO Blocked Inheritance

OU Name	Container Type	Inheritance Blocked	Path
fortinet ems	OU	Yes	pharmax.local/Fortinet EMS
linuxmachines	OU	Yes	pharmax.local/LinuxMachines

Table 48 - Blocked Inheritance GPO - PHARMAX.LOCAL

Health Check:

Corrective Actions: Review use of enforcement and blocked policy inheritance in Active Directory.

1.3 Domain Name System Summary

The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols.

1.3.1 PHARMAX.LOCAL Root Domain DNS Configuration

The following section provides a configuration summary of the DNS service.

1.3.1.1 Infrastructure Summary

The following section provides a summary of the DNS Infrastructure configuration.

DC Name	Build Number	IPv6	DnsSec	ReadOnly DC	Listening IP
SERVER-DC-01V	17763	Yes	No	No	192.168.5.1

Table 49 - Infrastructure Summary - PHARMAX.LOCAL

1.3.1.1.1 Forwarder Options

Microsoft Active Directory As Built Report - v1.0

DC Name	IP Address	Timeout	Use Root Hint	Use Recursion
SERVER-DC-01V	8.8.8.8	3/s	Yes	Yes
	10.0.0.138			

Table 50 - Forwarders - PHARMAX.LOCAL

1.3.1.2 SERVER-DC-01V DNS Zones

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
_msdcs.pharmax.local	Primary	Forest	Secure	Yes	No	No
acad.pharmax.local	Secondary	-	-	No	No	-
pharmax.local	Primary	Domain	Secure	Yes	No	No
TrustAnchors	Primary	Forest	None	Yes	No	No
uia.local	Stub	Domain	-	Yes	No	-
zenprsolutions.local	Stub	Domain	-	Yes	No	-

Table 51 - Zones - PHARMAX.LOCAL

1.3.1.2.1 Reverse Lookup Zone

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
0.in-addr.arpa	Primary	None	None	No	No	No
10.10.in-addr.arpa	Primary	Domain	Secure	Yes	No	No
127.in-addr.arpa	Primary	None	None	No	No	No
168.192.in-addr.arpa	Primary	Domain	Secure	Yes	No	No
23.172.in-addr.arpa	Primary	Domain	Secure	Yes	No	No
255.in-addr.arpa	Primary	None	None	No	No	No
70.23.172.in-addr.arpa	Primary	Forest	Secure	Yes	No	No

Table 52 - Zones - PHARMAX.LOCAL

1.3.1.2.2 Conditional Forwarder

Zone Name	Zone Type	Replication Scope	Master Servers	DS Integrated
b12.local	Forwarder	Forest	10.10.30.1	Yes
zenprsolutions.gov	Forwarder	Domain	8.8.8.8	Yes

Table 53 - Conditional Forwarders - PHARMAX.LOCAL

1.4 Dynamic Host Configuration Protocol Summary

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client/server architecture.

1.4.1 PHARMAX.LOCAL Root Domain DHCP Configuration

The following section provides a summary of the Dynamic Host Configuration Protocol.

1.4.1.1 DHCP Servers In Active Directory

The following section provides a summary of the DHCP servers information on PHARMAX.LOCAL.

DC Name	IP Address	Domain Name	Domain Joined	Authorized	Conflict Detection Attempts
cayey-dc-01v	10.10.33.1	pharmax.local	Yes	Yes	0
server-dc-01v	192.168.5.1	pharmax.local	Yes	Yes	1

Table 54 - DHCP Servers In Active Directory - PHARMAX.LOCAL

1.4.1.1.1 Service Database

DC Name	File Path	Backup Path	Backup Interval	Logging Enabled
cayey-dc-01v	C:\Windows\system32\dhcp\dhcp.mdb	C:\Windows\system32\dhcp\backup	60 min	Yes
server-dc-01v	C:\Windows\system32\dhcp\dhcp.mdb	C:\Windows\system32\dhcp\backup	60 min	Yes

Table 55 - DHCP Servers Database - PHARMAX.LOCAL

1.4.1.1.2 Dynamic DNS credentials

DC Name	User Name	Domain Name
cayey-dc-01v	-	-
server-dc-01v	administrator	PHARMAX.LOCAL

Table 56 - DHCP Servers Dynamic DNS Credentials - PHARMAX.LOCAL

Health Check:

Best Practice: Credentials for DNS update should be configured if secure dynamic DNS update is enabled and the domain controller is on the same host as the DHCP server.

1.4.1.2 IPv4 Scope Configuration

The following section provides a IPv4 configuration summary of the Dynamic Host Configuration Protocol.

1.4.1.2.1 IPv4 Service Statistics

DC Name	Total Scopes	Total Addresses	Addresses In Use	Addresses Available	Percentage In Use	Percentage Available
cayey-dc-01v	0	0	0	0	0	0
server-dc-01v	10	2118	125	1993	6	94

Table 57 - DHCP Server IPv4 Statistics - PHARMAX.LOCAL

1.4.1.2.2 SERVER-DC-01V IPv4 Scopes

The following section provides detailed information of the IPv4 Scope configuration.

Scope Id	Scope Name	Scope Range	Lease Duration	State
10.10.32.0/24	ESXi-vMotion-DR	10.10.32.10 - 10.10.32.250	8.00:00:00	Active
10.10.33.0/24	ESX-VM-NETWORK-DR	10.10.33.40 - 10.10.33.253	100.00:00:00	Active
10.10.34.0/24	ESXi-ISCSI-BLOCK-A-DR	10.10.34.10 - 10.10.34.253	8.00:00:00	Active
10.10.35.0/24	ESXi-ISCSI-BLOCK-B-DR	10.10.35.10 - 10.10.35.253	8.00:00:00	Active
192.168.10.0/24	ESX-vSAN-NET	192.168.10.10 - 192.168.10.253	8.00:00:00	Active
192.168.12.0/24	ESXi-ISCSI-BLOCK-B	192.168.12.10 - 192.168.12.240	8.00:00:00	Active
192.168.2.0/24	ESXi-vMotion	192.168.2.10 - 192.168.2.253	8.00:00:00	Active
192.168.4.0/24	ESXi-NFS-File	192.168.4.10 - 192.168.4.20	8.00:00:00	Active
192.168.6.0/24	ESXi-ISCSI-BLOCK-A	192.168.6.10 - 192.168.6.240	8.00:00:00	Active
192.168.7.0/24	ESX-VM-NETWORK	192.168.7.40 - 192.168.7.253	8.00:00:00	Active

Table 58 - IPv4 Scopes - SERVER-DC-01V

1.4.1.2.2.1 IPv4 Scope Statistics

Scope Id	Free IP	In Use IP	Percentage In Use	Reserved IP
10.10.32.0	241	0	0	0

Scope Id	Free IP	In Use IP	Percentage In Use	Reserved IP
10.10.33.0	212	2	1	3
10.10.34.0	242	2	1	0
10.10.35.0	242	2	1	0
192.168.10.0	244	0	0	0
192.168.12.0	224	7	3	3
192.168.2.0	242	2	1	0
192.168.4.0	11	0	0	0
192.168.6.0	223	8	3	2
192.168.7.0	112	102	48	17

Table 59 - IPv4 Scope Statistics - SERVER-DC-01V

1.4.1.2.2.2 IPv4 Network Interface Binding

Interface Alias	IP Address	Subnet Mask	State
Ethernet0	192.168.5.1	255.255.255.0	Enabled

Table 60 - IPv4 Network Interface binding - SERVER-DC-01V

1.4.1.3 IPv6 Scope Configuration

The following section provides a IPv6 configuration summary of the Dynamic Host Configuration Protocol.

1.4.1.3.1 IPv6 Service Statistics

DC Name	Total Scopes	Total Addresses	Addresses In Use	Addresses Available	Percentage In Use	Percentage Available
cayey-dc-01v	0	0	0	0	0	0
server-dc-01v	0	0	0	0	0	0

Table 61 - DHCP Server IPv6 Statistics - PHARMAX.LOCAL

1.5 Certificate Authority Summary

In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 or EMV standard.

Microsoft Active Directory As Built Report - v1.0

CA Name	Server Name	Type	Status
acad-ACADE-DC-01V-CA	ACADE-DC-01V	Enterprise Subordinate CA	Running
pharmax-CAYEY-DC-01V-CA	CAYEY-DC-01V	Enterprise Subordinate CA	Running
pharmax-SERVER-DC-01V-CA	SERVER-DC-01V	Enterprise Root CA	Running

Table 62 - Certification Authority - PHARMAX.LOCAL

1.5.1 Enterprise Root Certificate Authority

The following section provides the Enterprise Root CA information.

CA Name	pharmax-SERVER-DC-01V-CA
Server Name	SERVER-DC-01V
Type	Enterprise Root CA
Config String	Server-DC-01V.pharmax.local\pharmax-SERVER-DC-01V-CA
Operating System	Microsoft Windows Server 2019 Standard
Certificate	<p>[Subject] CN=pharmax-SERVER-DC-01V-CA, DC=pharmax, DC=local</p> <p>[Issuer] CN=pharmax-SERVER-DC-01V-CA, DC=pharmax, DC=local</p> <p>[Serial Number] 5D2E25D9AFFDE4904A05D70BEB7ACBD2</p> <p>[Not Before] 1/25/2020 7:35:16 PM</p> <p>[Not After] 1/25/2025 7:45:15 PM</p> <p>[Thumbprint] 0F6D4D3B8C71290E76B6B6C0661275F6F37B9CE0</p>
Status	Running

Table 63 - Enterprise Root CA - PHARMAX.LOCAL

1.5.2 Enterprise Subordinate Certificate Authority

The following section provides the Enterprise Subordinate CA information.

CA Name	acad-ACADE-DC-01V-CA
Server Name	ACADE-DC-01V

Microsoft Active Directory As Built Report - v1.0

Type	Enterprise Subordinate CA
Config String	acad-dc-01v.acad.pharmax.local\acad-ACADE-DC-01V-CA
Operating System	Microsoft Windows Server 2019 Standard Evaluation
Certificate	<p>[Subject] CN=acad-ACADE-DC-01V-CA, DC=acad, DC=pharmax, DC=local</p> <p>[Issuer] CN=pharmax-SERVER-DC-01V-CA, DC=pharmax, DC=local</p> <p>[Serial Number] 61000000F5B20F8367F4837C6A0000000000F5</p> <p>[Not Before] 9/22/2021 8:59:36 PM</p> <p>[Not After] 9/22/2023 9:09:36 PM</p> <p>[Thumbprint] 89532761827821E1B102CC8B86C529A6D2E92AC6</p>
Status	Running

Table 64 - Enterprise Subordinate CA - acad-ACADE-DC-01V-CA

CA Name	pharmax-CAYEY-DC-01V-CA
Server Name	CAYEY-DC-01V
Type	Enterprise Subordinate CA
Config String	cayey-dc-01v.pharmax.local\pharmax-CAYEY-DC-01V-CA
Operating System	Microsoft Windows Server 2019 Standard Evaluation
Certificate	<p>[Subject] CN=pharmax-CAYEY-DC-01V-CA, DC=pharmax, DC=local</p> <p>[Issuer] CN=pharmax-SERVER-DC-01V-CA, DC=pharmax, DC=local</p> <p>[Serial Number] 61000000F60DE0C8AB312FB51E0000000000F6</p> <p>[Not Before] 10/4/2021 10:33:08 AM</p> <p>[Not After] 10/4/2023 10:43:08 AM</p> <p>[Thumbprint]</p>

	CB2AC03DDA5A793DACAFC1EDC048CB1123D94B4B
Status	Running

Table 65 - Enterprise Subordinate CA - pharmax-CAYEY-DC-01V-CA

1.5.3 pharmax-SERVER-DC-01V-CA Details

1.5.3.1 Certificate Validity Period

The following section provides the Certification Authority Certificate Validity Period information.

CA Name	pharmax-SERVER-DC-01V-CA
Server Name	Server-DC-01V.pharmax.local
Validity Period	2 Years

Table 66 - Certificate Validity Period - PHARMAX.LOCAL

1.5.3.2 Access Control List (ACL)

DC Name	Owner	Group
pharmax-SERVER-DC-01V-CA	BUILTIN\Administrators	BUILTIN\Administrators

Table 67 - Access Control List - PHARMAX.LOCAL

1.5.3.2.1 Access Rights

Identity	Access Control Type	Rights
BUILTIN\Administrators	Allow	ManageCA, ManageCertificates
NT AUTHORITY\Authenticated Users	Allow	Enroll
PHARMAX\Domain Admins	Allow	ManageCA, ManageCertificates
PHARMAX\Enterprise Admins	Allow	ManageCA, ManageCertificates
PHARMAX\jocolon	Allow	ManageCA, ManageCertificates, Read, Enroll

Table 68 - Access Rights - pharmax-SERVER-DC-01V-CA

1.5.3.3 Cryptography Configuration

The following section provides the Certification Authority Cryptography Configuration information.

CA Name	pharmax-SERVER-DC-01V-CA
Server Name	SERVER-DC-01V

PublicKey Algorithm	RSA
Hashing Algorithm	SHA256
Provider Name	Microsoft Software Key Storage Provider
Alternate Signature Algorithm	No
Provider Is CNG	Yes

Table 69 - Cryptography Configuration - PHARMAX.LOCAL

1.5.3.4 Authority Information Access (AIA)

The following section provides the Certification Authority Authority Information Access information.

Reg URI	1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt
Config URI	1:C:\Windows\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaName> <CertificateName>.crt
Flags	1
Server Publish	Yes
Include To Extension	No
OCSP	No

Table 70 - Authority Information Access - pharmax-SERVER-DC-01V-CA

Reg URI	3:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11
Config URI	3:ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=Services,<ConfigurationContainer> <CAObjectClass>
Flags	1, 2
Server Publish	Yes
Include To Extension	Yes
OCSP	No

Table 71 - Authority Information Access - pharmax-SERVER-DC-01V-CA

Reg URI	0:http://%1/CertEnroll/%1_%3%4.crt
Config URI	0:http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName> <CertificateName>.crt
Flags	-
Server Publish	No
Include To Extension	No
OCSP	No

Table 72 - Authority Information Access - pharmax-SERVER-DC-01V-CA

Reg URI	0:file://%1/CertEnroll/%1_%3%4.crt
Config URI	0:file://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName> <CertificateName>.crt

Flags	-
Server Publish	No
Include To Extension	No
OCSP	No

Table 73 - Authority Information Access - pharmax-SERVER-DC-01V-CA

Reg URI	2:http://acade-dc-01v.acad.pharmax.local/CertData/%1_%3%4.crt
Config URI	2:http://acade-dc-01v.acad.pharmax.local/CertData/<ServerDNSName>_<CaName> <CertificateName>.crt
Flags	2
Server Publish	No
Include To Extension	Yes
OCSP	No

Table 74 - Authority Information Access - pharmax-SERVER-DC-01V-CA

1.5.3.5 Certificate Revocation List (CRL)

The following section provides the Certification Authority CRL Distribution Point information.

1.5.3.5.1 CRL Validity Period

CA Name	Base CRL	Base CRL Overlap	Delta CRL	Delta CRL Overlap
pharmax-SERVER-DC-01V-CA	50 Weeks	0 Hours	0 Days	0 Minutes

Table 75 - CRL Validity Period - PHARMAX.LOCAL

1.5.3.5.2 CRL Flags Settings

CA Name	Server Name	CRL Flags
pharmax-SERVER-DC-01V-CA	SERVER-DC-01V	DeleteExpiredCRLs

Table 76 - CRL Flags - PHARMAX.LOCAL

1.5.3.5.3 CRL Distribution Point

The following section provides the Certification Authority CRL Distribution Point information.

Reg URI	65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl
---------	--

Microsoft Active Directory As Built Report - v1.0

Config URI	65:C:\Windows\system32\CertSrv\CertEnroll\<CaName> <CRLNameSuffix> <DeltaCRLAllowed> .crl
Url Scheme	Unknown
ProjectedURI	65:C:\Windows\system32\CertSrv\CertEnroll\pharmax-SERVER-DC-01V-CA.crl 65:C:\Windows\system32\CertSrv\CertEnroll\pharmax-SERVER-DC-01V-CA+.crl
Flags	1, 64
CRL Publish	-
Delta CRL Publish	Yes
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 77 - CRL Distribution Point - pharmax-SERVER-DC-01V-CA

Reg URI	79:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
Config URI	79:ldap:///CN= <CATruncatedName> <CRLNameSuffix>,CN= <ServerShortName>,CN=CDP,CN=Public Key Services,CN=Services,<ConfigurationContainer> <CDPObjectClass>
Url Scheme	LDAP
ProjectedURI	79:ldap:///CN=pharmax-SERVER-DC-01V-CA,CN=Server-DC-01V,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=pharmax,DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint
Flags	1, 2, 4, 8, 64
CRL Publish	-
Delta CRL Publish	Yes
Add To Cert CDP	Yes
Add To Fresh est CRL	Yes
Add To Crl cdp	Yes

Table 78 - CRL Distribution Point - pharmax-SERVER-DC-01V-CA

Reg URI	0:http://%1/CertEnroll/%3%8%9.crl
Config URI	0:http://<ServerDNSName>/CertEnroll/<CaName> <CRLNameSuffix> <DeltaCRLAllowed> .crl
Url Scheme	HTTP
ProjectedURI	0:http:///CertEnroll/pharmax-SERVER-DC-01V-CA.crl 0:http:///CertEnroll/pharmax-SERVER-DC-01V-CA+.crl
Flags	-
CRL Publish	-
Delta CRL Publish	No

Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 79 - CRL Distribution Point - pharmax-SERVER-DC-01V-CA

Reg URI	0:file:///1/CertEnroll/%3%8%9.crl
Config URI	0:file:/// <ServerDNSName> /CertEnroll/<CaName> <CRLNameSuffix> <DeltaCRLAllowed> .crl
Url Scheme	UNC
ProjectedURI	0:file:///CertEnroll/pharmax-SERVER-DC-01V-CA.crl 0:file:///CertEnroll/pharmax-SERVER-DC-01V-CA+.crl
Flags	-
CRL Publish	-
Delta CRL Publish	No
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 80 - CRL Distribution Point - pharmax-SERVER-DC-01V-CA

Reg URI	6:http://acade-dc-01v.acad.pharmax.local/CertData/%3%8%9.crl
Config URI	6:http://acade-dc-01v.acad.pharmax.local/CertData/<CaName> <CRLNameSuffix> <DeltaCRLAllowed> .crl
Url Scheme	HTTP
ProjectedURI	6:http://acade-dc-01v.acad.pharmax.local/CertData/pharmax-SERVER-DC-01V-CA.crl 6:http://acade-dc-01v.acad.pharmax.local/CertData/pharmax-SERVER-DC-01V-CA+.crl
Flags	2, 4
CRL Publish	-
Delta CRL Publish	No
Add To Cert CDP	Yes
Add To Fresh est CRL	Yes
Add To Crl cdp	No

Table 81 - CRL Distribution Point - pharmax-SERVER-DC-01V-CA

1.5.3.6 AIA and CDP Health Status

Microsoft Active Directory As Built Report - v1.0

The following section is intended to perform Certification Authority health status checking by CA certificate chain status and validating all CRL Distribution Point (CDP) and Authority Information Access (AIA) URLs for each certificate in the chain.

CA Name	Childs	Health
pharmax-SERVER-DC-01V-CA	pharmax-SERVER-DC-01V-CA	Error

Table 82 - Certification Authority Health - PHARMAX.LOCAL

1.5.3.7 Certificate Template Summary

The following section provides the certificate templates that are assigned to a specified Certification Authority (CA). CA server can issue certificates only based on assigned templates.

Template Name	Schema Version	Supported CA	Autoenrollment
Administrator	1	Windows 2000 Server	No
Basic EFS	1	Windows 2000 Server	No
Computer	1	Windows 2000 Server	No
ConfigMgr Client Distribution	2	Windows Server 2003 Enterprise Edition	Yes
Directory Email Replication	2	Windows Server 2003 Enterprise Edition	Yes
Domain Controller	1	Windows 2000 Server	No
Domain Controller Authentication	2	Windows Server 2003 Enterprise Edition	Yes
EFS Recovery Agent	1	Windows 2000 Server	No
Kerberos Authentication	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Key Recovery Agent	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Labs Key Archive	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Web Server	2	Windows Server 2003 Enterprise Edition	No
Pharmax Workstation Authentication	2	Windows Server 2003 Enterprise Edition	Yes
Subordinate Certification Authority	1	Windows 2000 Server	No
User	1	Windows 2000 Server	No
Web Server	1	Windows 2000 Server	No
Web Server - ADFS	2	Windows Server 2003 Enterprise Edition	No
Web Server - Horizon	2	Windows Server 2003 Enterprise Edition	No

Microsoft Active Directory As Built Report - v1.0

Template Name	Schema Version	Supported CA	Autoenrollment
Web Server - Parallel	2	Windows Server 2003 Enterprise Edition	No
Web Server - WSUS SSL	2	Windows Server 2003 Enterprise Edition	No

Table 83 - Issued Certificate Template - pharmax-SERVER-DC-01V-CA

1.5.3.7.1 Certificate Template In Active Directory

The following section provides registered certificate templates from Active Directory.

Template Name	Schema Version	Supported CA	Autoenrollment
Administrator	1	Windows 2000 Server	No
Authenticated Session	1	Windows 2000 Server	No
Basic EFS	1	Windows 2000 Server	No
CA Exchange	2	Windows Server 2003 Enterprise Edition	No
CEP Encryption	1	Windows 2000 Server	No
Code Signing	1	Windows 2000 Server	No
Computer	1	Windows 2000 Server	No
ConfigMgr Client Distribution	2	Windows Server 2003 Enterprise Edition	Yes
Cross Certification Authority	2	Windows Server 2003 Enterprise Edition	No
Directory Email Replication	2	Windows Server 2003 Enterprise Edition	Yes
Domain Controller	1	Windows 2000 Server	No
Domain Controller Authentication	2	Windows Server 2003 Enterprise Edition	Yes
EFS Recovery Agent	1	Windows 2000 Server	No
Enrollment Agent	1	Windows 2000 Server	No
Enrollment Agent (Computer)	1	Windows 2000 Server	No
Exchange Enrollment Agent (Offline request)	1	Windows 2000 Server	No
Exchange Signature Only	1	Windows 2000 Server	No
Exchange User	1	Windows 2000 Server	No
IPSec	1	Windows 2000 Server	No
IPSec (Offline request)	1	Windows 2000 Server	No
Kerberos Authentication	2	Windows Server 2003 Enterprise Edition	Yes

Template Name	Schema Version	Supported CA	Autoenrollment
Key Recovery Agent	2	Windows Server 2003 Enterprise Edition	Yes
OCSP Response Signing	3	Windows Server 2008 Enterprise Edition	No
Pharmax Key Recovery Agent	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Labs Key Archive	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Web Server	2	Windows Server 2003 Enterprise Edition	No
Pharmax Workstation Authentication	2	Windows Server 2003 Enterprise Edition	Yes
RAS and IAS Server	2	Windows Server 2003 Enterprise Edition	Yes
Root Certification Authority	1	Windows 2000 Server	No
Router (Offline request)	1	Windows 2000 Server	No
Smartcard Logon	1	Windows 2000 Server	No
Smartcard User	1	Windows 2000 Server	No
Subordinate Certification Authority	1	Windows 2000 Server	No
Trust List Signing	1	Windows 2000 Server	No
User	1	Windows 2000 Server	No
User Signature Only	1	Windows 2000 Server	No
Web Server	1	Windows 2000 Server	No
Web Server - ADFS	2	Windows Server 2003 Enterprise Edition	No
Web Server - Horizon	2	Windows Server 2003 Enterprise Edition	No
Web Server - Parallel	2	Windows Server 2003 Enterprise Edition	No
Web Server - WSUS SSL	2	Windows Server 2003 Enterprise Edition	No
Workstation Authentication	2	Windows Server 2003 Enterprise Edition	Yes

Table 84 - Certificate Template in AD - PHARMAX.LOCAL

1.5.3.8 Key Recovery Agent Certificate

The following section provides the Key Recovery Agent certificate used to encrypt user's certificate private key and store it in CA database. In the case when user cannot access his or her certificate private key it is possible to recover it by Key Recovery Agent if Key Archival procedure was taken against particular certificate.

CA Name	pharmax-SERVER-DC-01V-CA
Server Name	SERVER-DC-01V
Certificate	[Subject] CN=Administrator, CN=Users, DC=pharmax, DC=local [Issuer] CN=pharmax-SERVER-DC-01V-CA, DC=pharmax, DC=local [Serial Number] 61000001068FABBB1D8B7B986A000000000106 [Not Before] 11/16/2021 8:11:55 PM [Not After] 11/16/2023 8:11:55 PM [Thumbprint] 0C65947128A94A0209907127D13F81AD5840CA37

Table 85 - Key Recovery Agent Certificate - pharmax-SERVER-DC-01V-CA

1.5.4 acad-ACADE-DC-01V-CA Details

1.5.4.1 Certificate Validity Period

The following section provides the Certification Authority Certificate Validity Period information.

CA Name	acad-ACADE-DC-01V-CA
Server Name	acad-dc-01v.acad.pharmax.local
Validity Period	2 Years

Table 86 - Certificate Validity Period - PHARMAX.LOCAL

1.5.4.2 Access Control List (ACL)

DC Name	Owner	Group
acad-ACADE-DC-01V-CA	BUILTIN\Administrators	BUILTIN\Administrators

Table 87 - Access Control List - PHARMAX.LOCAL

1.5.4.2.1 Access Rights

Microsoft Active Directory As Built Report - v1.0

Identity	Access Control Type	Rights
ACAD\Domain Admins	Allow	ManageCA, ManageCertificates
BUILTIN\Administrators	Allow	ManageCA, ManageCertificates
NT AUTHORITY\Authenticated Users	Allow	Enroll
PHARMAX\Enterprise Admins	Allow	ManageCA, ManageCertificates

Table 88 - Access Rights - acad-ACADE-DC-01V-CA

1.5.4.3 Cryptography Configuration

The following section provides the Certification Authority Cryptography Configuration information.

CA Name	acad-ACADE-DC-01V-CA
Server Name	ACADE-DC-01V
PublicKey Algorithm	RSA
Hashing Algorithm	SHA256
Provider Name	Microsoft Software Key Storage Provider
Alternate Signature Algorithm	No
Provider Is CNG	Yes

Table 89 - Cryptography Configuration - PHARMAX.LOCAL

1.5.4.4 Authority Information Access (AIA)

The following section provides the Certification Authority Authority Information Access information.

Reg URI	1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt
Config URI	1:C:\Windows\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaName><CertificateName>.crt
Flags	1
Server Publish	Yes
Include To Extension	No
OCSP	No

Table 90 - Authority Information Access - acad-ACADE-DC-01V-CA

Reg URI	3:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11
Config URI	3:ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=Services,<ConfigurationContainer><CAObjectClass>
Flags	1, 2
Server Publish	Yes
Include To Extension	Yes

OCSP	No
------	----

Table 91 - Authority Information Access - acad-ACADE-DC-01V-CA

Reg URI	0:http://%1/CertEnroll/%1_%3%4.crt
Config URI	0:http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt
Flags	-
Server Publish	No
Include To Extension	No
OCSP	No

Table 92 - Authority Information Access - acad-ACADE-DC-01V-CA

Reg URI	0:file://%1/CertEnroll/%1_%3%4.crt
Config URI	0:file://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt
Flags	-
Server Publish	No
Include To Extension	No
OCSP	No

Table 93 - Authority Information Access - acad-ACADE-DC-01V-CA

Reg URI	2:http://acad-dc-01v.acad.pharmax.local/CertEnroll/%1_%3%4.crt
Config URI	2:http://acad-dc-01v.acad.pharmax.local/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt
Flags	2
Server Publish	No
Include To Extension	Yes
OCSP	No

Table 94 - Authority Information Access - acad-ACADE-DC-01V-CA

Reg URI	32:http://acad-dc-01v.acad.pharmax.local/ocsp
Config URI	32:http://acad-dc-01v.acad.pharmax.local/ocsp
Flags	32
Server Publish	No
Include To Extension	No
OCSP	Yes

Table 95 - Authority Information Access - acad-ACADE-DC-01V-CA

1.5.4.5 Certificate Revocation List (CRL)

The following section provides the Certification Authority CRL Distribution Point information.

1.5.4.5.1 CRL Validity Period

CA Name	Base CRL	Base CRL Overlap	Delta CRL	Delta CRL Overlap
acad-ACADE-DC-01V-CA	1 Weeks	0 Hours	1 Days	0 Minutes

Table 96 - CRL Validity Period - PHARMAX.LOCAL

1.5.4.5.2 CRL Flags Settings

CA Name	Server Name	CRL Flags
acad-ACADE-DC-01V-CA	ACADE-DC-01V	DeleteExpiredCRLs

Table 97 - CRL Flags - PHARMAX.LOCAL

1.5.4.5.3 CRL Distribution Point

The following section provides the Certification Authority CRL Distribution Point information.

Reg URI	65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl
Config URI	65:C:\Windows\system32\CertSrv\CertEnroll\<CaName> <CRLNameSuffix> <DeltaCRLAllowed>.crl
Url Scheme	Unknown
ProjectedURI	65:C:\Windows\system32\CertSrv\CertEnroll\acad-ACADE-DC-01V-CA.crl 65:C:\Windows\system32\CertSrv\CertEnroll\acad-ACADE-DC-01V-CA+.crl
Flags	1, 64
CRL Publish	-
Delta CRL Publish	Yes
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 98 - CRL Distribution Point - acad-ACADE-DC-01V-CA

Reg URI	79:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
Config URI	79:ldap:///CN=<CATruncatedName> <CRLNameSuffix>,CN=<ServerShortName>,CN=CDP,CN=Public Key Services,CN=Services,<ConfigurationContainer> <CDPObjectClass>
Url Scheme	LDAP

Microsoft Active Directory As Built Report - v1.0

ProjectedURI	79:ldap:///CN=acad-ACADE-DC-01V-CA,CN=acade-dc-01v,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=pharmax,DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint
Flags	1, 2, 4, 8, 64
CRL Publish	-
Delta CRL Publish	Yes
Add To Cert CDP	Yes
Add To Fresh est CRL	Yes
Add To Crl cdp	Yes

Table 99 - CRL Distribution Point - acad-ACADE-DC-01V-CA

Reg URI	0:http://%1/CertEnroll/%3%8%9.crl
Config URI	0:http://<ServerDNSName>/CertEnroll/<CaName> <CRLNameSuffix> <DeltaCRLAllowed>.crl
Url Scheme	HTTP
ProjectedURI	0:http:///CertEnroll/acad-ACADE-DC-01V-CA.crl 0:http:///CertEnroll/acad-ACADE-DC-01V-CA+.crl
Flags	-
CRL Publish	-
Delta CRL Publish	No
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 100 - CRL Distribution Point - acad-ACADE-DC-01V-CA

Reg URI	0:file://%1/CertEnroll/%3%8%9.crl
Config URI	0:file://<ServerDNSName>/CertEnroll/<CaName> <CRLNameSuffix> <DeltaCRLAllowed>.crl
Url Scheme	UNC
ProjectedURI	0:file:///CertEnroll/acad-ACADE-DC-01V-CA.crl 0:file:///CertEnroll/acad-ACADE-DC-01V-CA+.crl
Flags	-
CRL Publish	-
Delta CRL Publish	No
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 101 - CRL Distribution Point - acad-ACADE-DC-01V-CA

Reg URI	6:http://acade-dc-01v.acad.pharmax.local/CertEnroll/%3%8%9.crl
---------	--

Config URI	6:http://acad-dc-01v.acad.pharmax.local/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
Url Scheme	HTTP
ProjectedURI	6:http://acad-dc-01v.acad.pharmax.local/CertEnroll/acad-ACADE-DC-01V-CA.crl 6:http://acad-dc-01v.acad.pharmax.local/CertEnroll/acad-ACADE-DC-01V-CA+.crl
Flags	2, 4
CRL Publish	-
Delta CRL Publish	No
Add To Cert CDP	Yes
Add To Fresh est CRL	Yes
Add To Crl cdp	No

Table 102 - CRL Distribution Point - acad-ACADE-DC-01V-CA

1.5.4.6 AIA and CDP Health Status

The following section is intended to perform Certification Authority health status checking by CA certificate chain status and validating all CRL Distribution Point (CDP) and Authority Information Access (AIA) URLs for each certificate in the chain.

CA Name	Childs	Health
acad-ACADE-DC-01V-CA	acad-ACADE-DC-01V-CA pharmax-SERVER-DC-01V-CA	Error

Table 103 - Certification Authority Health - PHARMAX.LOCAL

1.5.4.7 Certificate Template Summary

The following section provides the certificate templates that are assigned to a specified Certification Authority (CA). CA server can issue certificates only based on assigned templates.

Template Name	Schema Version	Supported CA	Autoenrollment
Administrator	1	Windows 2000 Server	No
Basic EFS	1	Windows 2000 Server	No
Computer	1	Windows 2000 Server	No
Directory Email Replication	2	Windows Server 2003 Enterprise Edition	Yes
Domain Controller	1	Windows 2000 Server	No
Domain Controller Authentication	2	Windows Server 2003 Enterprise Edition	Yes

Template Name	Schema Version	Supported CA	Autoenrollment
EFS Recovery Agent	1	Windows 2000 Server	No
Kerberos Authentication	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Workstation Authentication	2	Windows Server 2003 Enterprise Edition	Yes
Subordinate Certification Authority	1	Windows 2000 Server	No
User	1	Windows 2000 Server	No
Web Server	1	Windows 2000 Server	No

Table 104 - Issued Certificate Template - acad-ACADE-DC-01V-CA

1.5.4.7.1 Certificate Template In Active Directory

The following section provides registered certificate templates from Active Directory.

Template Name	Schema Version	Supported CA	Autoenrollment
Administrator	1	Windows 2000 Server	No
Authenticated Session	1	Windows 2000 Server	No
Basic EFS	1	Windows 2000 Server	No
CA Exchange	2	Windows Server 2003 Enterprise Edition	No
CEP Encryption	1	Windows 2000 Server	No
Code Signing	1	Windows 2000 Server	No
Computer	1	Windows 2000 Server	No
ConfigMgr Client Distribution	2	Windows Server 2003 Enterprise Edition	Yes
Cross Certification Authority	2	Windows Server 2003 Enterprise Edition	No
Directory Email Replication	2	Windows Server 2003 Enterprise Edition	Yes
Domain Controller	1	Windows 2000 Server	No
Domain Controller Authentication	2	Windows Server 2003 Enterprise Edition	Yes
EFS Recovery Agent	1	Windows 2000 Server	No
Enrollment Agent	1	Windows 2000 Server	No
Enrollment Agent (Computer)	1	Windows 2000 Server	No
Exchange Enrollment Agent (Offline request)	1	Windows 2000 Server	No
Exchange Signature Only	1	Windows 2000 Server	No
Exchange User	1	Windows 2000 Server	No

Microsoft Active Directory As Built Report - v1.0

Template Name	Schema Version	Supported CA	Autoenrollment
IPSec	1	Windows 2000 Server	No
IPSec (Offline request)	1	Windows 2000 Server	No
Kerberos Authentication	2	Windows Server 2003 Enterprise Edition	Yes
Key Recovery Agent	2	Windows Server 2003 Enterprise Edition	Yes
OCS Response Signing	3	Windows Server 2008 Enterprise Edition	No
Pharmax Key Recovery Agent	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Labs Key Archive	2	Windows Server 2003 Enterprise Edition	Yes
Pharmax Web Server	2	Windows Server 2003 Enterprise Edition	No
Pharmax Workstation Authentication	2	Windows Server 2003 Enterprise Edition	Yes
RAS and IAS Server	2	Windows Server 2003 Enterprise Edition	Yes
Root Certification Authority	1	Windows 2000 Server	No
Router (Offline request)	1	Windows 2000 Server	No
Smartcard Logon	1	Windows 2000 Server	No
Smartcard User	1	Windows 2000 Server	No
Subordinate Certification Authority	1	Windows 2000 Server	No
Trust List Signing	1	Windows 2000 Server	No
User	1	Windows 2000 Server	No
User Signature Only	1	Windows 2000 Server	No
Web Server	1	Windows 2000 Server	No
Web Server - ADFS	2	Windows Server 2003 Enterprise Edition	No
Web Server - Horizon	2	Windows Server 2003 Enterprise Edition	No
Web Server - Parallel	2	Windows Server 2003 Enterprise Edition	No
Web Server - WSUS SSL	2	Windows Server 2003 Enterprise Edition	No
Workstation Authentication	2	Windows Server 2003 Enterprise Edition	Yes

Table 105 - Certificate Template in AD - PHARMAX.LOCAL

1.5.4.8 Key Recovery Agent Certificate

Microsoft Active Directory As Built Report - v1.0

The following section provides the Key Recovery Agent certificate used to encrypt user's certificate private key and store it in CA database. In the case when user cannot access his or her certificate private key it is possible to recover it by Key Recovery Agent if Key Archival procedure was taken against particular certificate.

CA Name	acad-ACADE-DC-01V-CA
Server Name	ACADE-DC-01V
Certificate	[Subject] CN=Administrator, CN=Users, DC=pharmax, DC=local [Issuer] CN=pharmax-SERVER-DC-01V-CA, DC=pharmax, DC=local [Serial Number] 610000011FC4B5F75727EEAB0800000000011F [Not Before] 1/23/2022 10:30:44 PM [Not After] 1/23/2024 10:30:44 PM [Thumbprint] 4883ED66CAB909725F89D7483E97DBF69C4CDA9B

Table 106 - Key Recovery Agent Certificate - acad-ACADE-DC-01V-CA

1.5.5 pharmax-CAYEY-DC-01V-CA Details

1.5.5.1 Certificate Validity Period

The following section provides the Certification Authority Certificate Validity Period information.

CA Name	pharmax-CAYEY-DC-01V-CA
Server Name	cayey-dc-01v.pharmax.local
Validity Period	2 Years

Table 107 - Certificate Validity Period - PHARMAX.LOCAL

1.5.5.2 Access Control List (ACL)

DC Name	Owner	Group
pharmax-CAYEY-DC-01V-CA	BUILTIN\Administrators	BUILTIN\Administrators

Table 108 - Access Control List - PHARMAX.LOCAL

1.5.5.2.1 Access Rights

Identity	Access Control Type	Rights
BUILTIN\Administrators	Allow	ManageCA, ManageCertificates
NT AUTHORITY\Authenticated Users	Allow	Enroll
PHARMAX\Domain Admins	Allow	ManageCA, ManageCertificates
PHARMAX\Enterprise Admins	Allow	ManageCA, ManageCertificates

Table 109 - Access Rights - pharmax-CAYEY-DC-01V-CA

1.5.5.3 Cryptography Configuration

The following section provides the Certification Authority Cryptography Configuration information.

CA Name	pharmax-CAYEY-DC-01V-CA
Server Name	CAYEY-DC-01V
PublicKey Algorithm	RSA
Hashing Algorithm	SHA256
Provider Name	Microsoft Software Key Storage Provider
Alternate Signature Algorithm	No
Provider Is CNG	Yes

Table 110 - Cryptography Configuration - PHARMAX.LOCAL

1.5.5.4 Authority Information Access (AIA)

The following section provides the Certification Authority Authority Information Access information.

Reg URI	1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt
Config URI	1:C:\Windows\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaName> <CertificateName>.crt
Flags	1
Server Publish	Yes
Include To Extension	No
OCSP	No

Table 111 - Authority Information Access - pharmax-CAYEY-DC-01V-CA

Reg URI	3:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11
Config URI	3:ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=Services,<ConfigurationContainer> <CAObjectClass>
Flags	1, 2

Microsoft Active Directory As Built Report - v1.0

Server Publish	Yes
Include To Extension	Yes
OCSP	No

Table 112 - Authority Information Access - pharmax-CAYEY-DC-01V-CA

Reg URI	0:http://%1/CertEnroll/%1_%3%4.crt
Config URI	0:http://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt
Flags	-
Server Publish	No
Include To Extension	No
OCSP	No

Table 113 - Authority Information Access - pharmax-CAYEY-DC-01V-CA

Reg URI	0:file://%1/CertEnroll/%1_%3%4.crt
Config URI	0:file://<ServerDNSName>/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt
Flags	-
Server Publish	No
Include To Extension	No
OCSP	No

Table 114 - Authority Information Access - pharmax-CAYEY-DC-01V-CA

1.5.5.5 Certificate Revocation List (CRL)

The following section provides the Certification Authority CRL Distribution Point information.

1.5.5.5.1 CRL Validity Period

CA Name	Base CRL	Base CRL Overlap	Delta CRL	Delta CRL Overlap
pharmax-CAYEY-DC-01V-CA	1 Weeks	0 Hours	1 Days	0 Minutes

Table 115 - CRL Validity Preriod - PHARMAX.LOCAL

1.5.5.5.2 CRL Flags Settings

CA Name	Server Name	CRL Flags
pharmax-CAYEY-DC-01V-CA	CAYEY-DC-01V	DeleteExpiredCRLs

Table 116 - CRL Flags - PHARMAX.LOCAL

1.5.5.5.3 CRL Distribution Point

The following section provides the Certification Authority CRL Distribution Point information.

Reg URI	65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl
Config URI	65:C:\Windows\system32\CertSrv\CertEnroll\<CaName> <CRLNameSuffix> <DeltaCRLAllowed>.crl
Url Scheme	Unknown
ProjectedURI	65:C:\Windows\system32\CertSrv\CertEnroll\pharmax-CAYEY-DC-01V-CA.crl 65:C:\Windows\system32\CertSrv\CertEnroll\pharmax-CAYEY-DC-01V-CA+.crl
Flags	1, 64
CRL Publish	-
Delta CRL Publish	Yes
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 117 - CRL Distribution Point - pharmax-CAYEY-DC-01V-CA

Reg URI	79:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10
Config URI	79:ldap:///CN= <CATruncatedName> <CRLNameSuffix>,CN= <ServerShortName>,CN=CDP,CN=Public Key Services,CN=Services,<ConfigurationContainer> <CDPObject Class>
Url Scheme	LDAP
ProjectedURI	79:ldap:///CN=pharmax-CAYEY-DC-01V-CA,CN=cayey-dc-01v,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=pharmax,DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint
Flags	1, 2, 4, 8, 64
CRL Publish	-
Delta CRL Publish	Yes
Add To Cert CDP	Yes
Add To Fresh est CRL	Yes
Add To Crl cdp	Yes

Table 118 - CRL Distribution Point - pharmax-CAYEY-DC-01V-CA

Reg URI	0:http://%1/CertEnroll/%3%8%9.crl
Config URI	0:http://<ServerDNSName>/CertEnroll/<CaName> <CRLNameSuffix> <DeltaCRLAllowed>.crl
Url Scheme	HTTP

ProjectedURI	0:http:///CertEnroll/pharmax-CAYEY-DC-01V-CA.crl 0:http:///CertEnroll/pharmax-CAYEY-DC-01V-CA+.crl
Flags	-
CRL Publish	-
Delta CRL Publish	No
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 119 - CRL Distribution Point - pharmax-CAYEY-DC-01V-CA

Reg URI	0:file:///1/CertEnroll/%3%8%9.crl
Config URI	0:file://<ServerDNSName>/CertEnroll/<CaName> <CRLNameSuffix> <DeltaCRLAllowed>.crl
Url Scheme	UNC
ProjectedURI	0:file:///CertEnroll/pharmax-CAYEY-DC-01V-CA.crl 0:file:///CertEnroll/pharmax-CAYEY-DC-01V-CA+.crl
Flags	-
CRL Publish	-
Delta CRL Publish	No
Add To Cert CDP	No
Add To Fresh est CRL	No
Add To Crl cdp	No

Table 120 - CRL Distribution Point - pharmax-CAYEY-DC-01V-CA

1.5.5.6 AIA and CDP Health Status

The following section is intended to perform Certification Authority health status checking by CA certificate chain status and validating all CRL Distribution Point (CDP) and Authority Information Access (AIA) URLs for each certificate in the chain.

CA Name	Childs	Health
pharmax-CAYEY-DC-01V-CA	pharmax-CAYEY-DC-01V-CA pharmax-SERVER-DC-01V-CA	Error

Table 121 - Certification Authority Health - PHARMAX.LOCAL