More Details www.AnoopCNair.com

Account Name	Use	Permission
AD Group Discovery Account	The AD Group Discovery Account is used to discover local, global, and universal security groups, the membership within these groups, and the membership within distribution groups from the specified locations in Active directory Domain Services. Distribution groups are not discovered as group resources.	This account can be a computer account of the site server that runs discovery, or a Windows user account. It must have Read access permission to the Active Directory locations that are specified for discovery.
AD System Discovery Account	The AD System Discovery Account is used to discover computers from the specified locations in Active Directory Domain Services.	This account can be a computer account of the site server that runs discovery, or a Windows user account. It must have Read access permission to the Active Directory locations that are specified for discovery.
AD User Discovery Account	The AD User Discovery Account is used to discover user accounts from the specified locations in Active Directory Domain Services.	This account can be a computer account of the site server that runs discovery, or a Windows user account. It must have Read access permission to the Active Directory locations that are specified for discovery.
AD Forest Account	The AD Forest Account is used to discovery network infrastructure from Active Directory forests, and is also used by central administration sites and primary sites to publish site data to the Active Directory Domain Services of a forest.	This account must have Read permissions to each Active Directory forest where you want to discover network infrastructure. This account must have **Full Control permissions** to the **System Management container** and all its child objects in each Active Directory forest where you want to publish site data.
AMT Provisioning and Discovery Account	The AMT Provisioning and Discovery Account is functionally equivalent to the AMT Remote Admin Account and resides in the Management Engine BIOS extension (MEBx) of Intel AMT-based computers. This account is used by the server that runs the out of band service point role to manage some network interface features of AMT, by using the out of band management feature.	The account is stored in the Management Engine BIOS extensions of the AMT-based computer and does not correspond to any account in Windows.
AMT Provisioning Removal Account	The AMT Provisioning Removal Account can remove AMT provisioning information if you have to recover the site. You might also be able to use it when a Configuration Manager client was reassigned and the AMT provisioning information was not removed from the computer in the old site.	To successfully remove the AMT provisioning information by using the AMT Provisioning Removal Account, all the following must be true: The AMT Provisioning Removal Account is configured in the out of band management component properties.The account that is configured for the AMT Provisioning Removal Account was configured as an AMT User Account in the out of band management component properties when the AMT-based computer was provisioned or updated. The account that is configured for the AMT Provisioning Removal Account must be a member of the local Administrators group on the out of band service point computer.The AMT auditing log is not enabled. Because this is a Windows user account, specify an account with a strong password that does not expire.
AMT Remote Admin Account	The AMT Remote Admin Account is the account in the Management Engine BIOS extension (MEBx) of Intel AMT-based computers that is used by the server running the out of band service point role to manage some network interface features of AMT in Configuration Manager, by using the out of band management feature.	Configuration Manager automatically sets the remote admin account password for computers that it provisions for AMT, and this is then used for subsequent authenticated access to the AMT firmware. This account is functionally equivalent to the Configuration Manager AMT Provisioning and Discovery Account.
AMT User Account	AMT User Accounts control which Windows users or groups can run management functions in the Out of Band Management console.	The configuration of the AMT User Accounts creates the equivalent of an access control list (ACL) in the AMT firmware. When the logged on user attempts to run the Out of Band Management console, AMT uses Kerberos to authenticate the account and then authorizes or denies access to run the AMT management functions.
AI Synchronization Point Proxy Server Account	The Asset Intelligence Synchronization Point Proxy Server Account is used by the Asset Intelligence synchronization point to access the Internet via a proxy server or firewall that requires authenticated access.	Specify an account that has the least possible permissions for the required proxy server or firewall.
Capture Operating System Image Account	The Capture Operating System Image Account is used by Configuration Manager to access the folder where captured images are stored when you deploy operating systems. This account is required if you add the step Capture Operating System Image to a task sequence.	The account must have Read and Write permissions on the network share where the captured image is stored. If the password the account is changed in Windows, you must update the task sequence with the new password. The Configuration Manager client will receive the new password when it next downloads client policy. If you use this account, you can create one domain user account with minimal permissions to access the required network resources and use it for all task sequence accounts.**Do not assign this account interactive logon permissions. Do not use the Network Access account for this account.**
Client Push Installation Account	The Client Push Installation Account is used to connect to computers and install the Configuration Manager client software if you deploy clients by using client push installation. If this account is not specified, the site server account is used to try to install the client software.	This account must be a member of the local Administrators group on the computers where the Configuration Manager client software is to be installed. This account does not require Domain Admin rights.**Do not grant this account the right to log on locally.**
Enrollment Point Connection Account	The Enrollment Point Connection Account connects the enrollment point to the Configuration Manager site database. By default, the computer account of the enrollment point is used, but you can configure a user account instead. You must specify a user account whenever the enrollment point is in an untrusted domain from the site server.	This account requires Read and Write access to the site database.
Exchange Server Connection Account	The Exchange Server Connection Account connects the site server to the specified Exchange Server computer to find and manage mobile devices that connect to Exchange Server.	This account requires Exchange PowerShell cmdlets that provide the required permissions to the Exchange Server computer.
Exchange Server Connector Proxy Server Account	The Exchange Server Connector Proxy Server Account is used by the Exchange Server connector to access the Internet via a proxy server or firewall that requires authenticated access.	Specify an account that has the least possible permissions for the required proxy server or firewall.
Endpoint Protection SMTP Server Connection Account	For Configuration Manager with no service pack: The Endpoint Protection SMTP Server Connection Account is used by the site server to send email alerts for Endpoint Protection when the SMTP server requires authenticated access.	Specify an account that has the least possible permissions to send emails.

Health State Reference Publishing Account	The Health State Reference Publishing Account is used to publish the Network Access Protection (NAP) health state reference for Configuration Manager to Active Directory Domain Services. If you do not configure an account, Configuration Manager attempts to use the site server computer account to publish the health state references.	This account requires Read, Write and Create permissions to the Active Directory forest that stores the health state reference. Create the account in the forest that is designated to store the health state references. Assign the least possible permissions to this account and do not use the same account that is specified for the Health State Reference Querying Account, which requires only Read permissions.
Health State Reference Querying Account	The Health State Reference Querying Account is used to retrieve the Network Access Protection (NAP) health state reference for Configuration Manager from Active Directory Domain Services. If you do not configure an account, Configuration Manager attempts to use the site server computer account to retrieve the health state references.	This account requires Read permissions to the Configuration Manager Systems Management container in the Global Catalog. Create the account in the forest that is designated to store the health state references. Do not use the same account for the Health State Reference Publishing Account, which requires more privileges.**Do not grant this account interactive logon rights.**
Management Point Database Connection Account	The Management Point Database Connection Account is used to connect the management point to the Configuration Manager site database so that it can send and retrieve information for clients. By default, the computer account of the management point is used, but you can configure a user account instead. You must specify a user account whenever the management point is in an untrusted domain from the site server.	Create the account as a low-rights, local account on the computer that runs Microsoft SQL Server.**Do not grant this account interactive logon rights.**
MEBx Account	The MEBx Account is the account in the Management Engine BIOS extension (MEBx) on Intel AMT-based computers and it is used for initial authenticated access to the AMT firmware on AMT-based computers.	The account is stored in the Management Engine BIOS extensions of the AMT-based computer. This account does not correspond to any account in Windows.If the default MEBx password has not been changed before Configuration Manager provisions the computer for AMT, during the AMT provisioning process, Configuration Manager sets the password that you configure.
Multicast Connection Account	The Multicast Connection Account is used by distribution points that are configured for multicast to read information from the site database. By default, the computer account of the distribution point is used, but you can configure a user account instead. You must specify a user account whenever the site database is in an untrusted forest. For example, if your data center has a perimeter network in a forest other than the site server and site database, you can use this account to read the multicast information from the site database.	If you create this account, create it as a low-rights, local account on the computer that runs Microsoft SQL Server.**Do not grant this account interactive logon rights.**
Network Access Account	The Network Access Account is used by client computers when they cannot use their local computer account to access content on distribution points. For example, this applies to workgroup clients and computers from untrusted domains. This account might also be used during operating system deployment when the computer installing the operating system does not yet have a computer account on the domain.	Grant this account the minimum appropriate permissions on the content that the client requires to access the software. The account must have the Access this computer from the network right on the distribution point or other server that holds the package content. Because you can create only one Network Access Account per site, this account must function for all packages and task sequences for which it is required. **Do not grant this account interactive logon rights. Do not grant this account the right to join computers to the domain. If you must join computers to the domain during a task sequence, use the Task Sequence Editor Domain Joining Account.**
Package Access Account	Package Access Accounts enable you to set NTFS permissions to specify the users and user groups that can access a package folder on distribution points. By default, Configuration Manager grants access only to the generic access accounts Users and Administrators, but you can control access for client computers by using additional Windows accounts or groups. Mobile devices always retrieve package content anonymously, so the Package Access Accounts are not used by mobile device.	When Configuration Manager creates the package share on a distribution point, it grants Read access to the local Users group and Full Control to the local Administrators group. The actual permissions required will depend on the package. If you have clients in workgroups or in untrusted forests, those clients use the Network Access Account to access the package content. Make sure that the Network Access Account has permissions to the package by using the defined Package Access Accounts.**You do not have to add the Network Access Account as a Package Access Account**
Reporting Services Point Account	The Reporting Services Point Account is used by SQL Server Reporting Services to retrieve the data for Configuration Manager reports from the site database.	The Windows user account and password that you specify are encrypted and stored in the SQL Server Reporting Services database.
Remote Tools Permitted Viewer Accounts	The accounts that you specify as Permitted Viewers for remote control are a list of users who are allowed to use remote tools functionality on clients.	
Site System Installation Account	The Site System Installation Account is used by the site server to install, reinstall, uninstall, and configure site systems. If you configure the site system to require the site server to initiate connections to this site system, Configuration Manager also uses this account to pull data from the site system computer after the site system and any site system roles are installed. Each site system can have a different Site System Installation Account, but you can configure only one Site System Installation Account to manage all site system roles on that site system.	This account requires local administrative permissions on the site systems that they will install and configure. Additionally, this account must have Access this computer from the network in the security policy on the site systems that they will install and configure.
SMTP Server Connection Account	For Configuration Manager SP1 only: The SMTP Server Connection Account is used by the site server to send email alerts when the SMTP server requires authenticated access.	Specify an account that has the least possible permissions to send emails.
Software Update Point Connection Account	The Software Update Point Connection Account is used by the site server for the following two software updates services: WSUS Configuration Manager, which configures settings such as product definitions, classifications, and upstream settings. WSUS Synchronization Manager, which requests synchronization to an upstream WSUS server or Microsoft Update. The Site System Installation Account can install components for software updates, but cannot perform software updates-specific functions on the software update point. If you cannot use the site server computer account for this functionality because the software update point is in an untrusted forest, you must specify this account in addition to the Site System Installation Account.	This account must be a local administrator on the computer where WSUS is installed, and be part of the local WSUS Administrators group.

Software Update Point Proxy Server Account	The Software Update Point Proxy Server Account is used by the software update point to access the Internet via a proxy server or firewall that requires authenticated access.	Specify an account that has the least possible permissions for the required proxy server or firewall.
Source Site Account	The Source Site Account is used by the migration process to access the SMS Provider of the source site. This account requires Read permissions to site objects in the source site to gather data for migration jobs. If you upgrade Configuration Manager 2007 distribution points or secondary sites that have co-located distribution points to System Center 2012 Configuration Manager distribution points, this account must also have Delete permissions to the Site class to successfully remove the distribution point from the Configuration Manager 2007 site during the upgrade.	Both the Source Site Account and Source Site Database Account are identified as Migration Manager in the Accounts node of the Administration workspace in the Configuration Manager console.
Source Site Database Account	The Source Site Database Account is used by the migration process to access the SQL Server database for the source site.	The Source Site Database Account is used by the migration process to access the SQL Server database for the source site. Both the Source Site Account and Source Site Database Account are identified as Migration Manager in the Accounts node of the Administration workspace in the Configuration Manager console.
Task Sequence Editor Domain Joining Account	The Task Sequence Editor Domain Joining Account is used in a task sequence to join a newly imaged computer to a domain. This account is required if you add the step Join Domain or Workgroup to a task sequence, and then select Join a domain. This account can also be configured if you add the step Apply Network Settings to a task sequence, but it is not required.	This account requires the Domain Join right in the domain that the computer will be joining.**Do not assign this account interactive logon permissions. Do not use the Network Access Account for this account.**
Task Sequence Editor Network Folder Connection Account	The Task Sequence Editor Network Folder Connection Account is used by a task sequence to connect to a shared folder on the network. This account is required if you add the step Connect to Network Folder to a task sequence.	This account requires permissions to access the specified shared folder and must be a user domain account.**Do not assign this account interactive logon permissions. Do not use the Network Access Account for this account.**
Task Sequence Run As Account	The Task Sequence Run As Account is used to run command lines in task sequences and use credentials other than the local system account. This account is required if you add the step Run Command Line to a task sequence but do not want the task sequence to run with Local System account permissions on the managed computer.	Configure the account to have the minimum permissions required to run the command line that specified in the task sequence. The account requires interactive login rights, and it usually requires the ability to install software and access network resources.