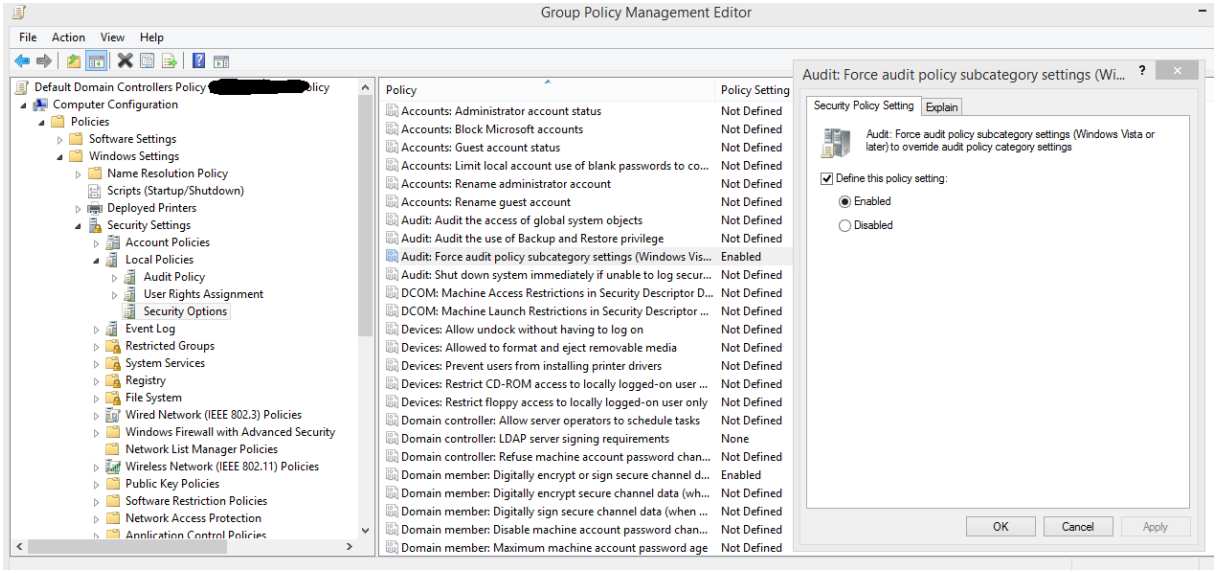
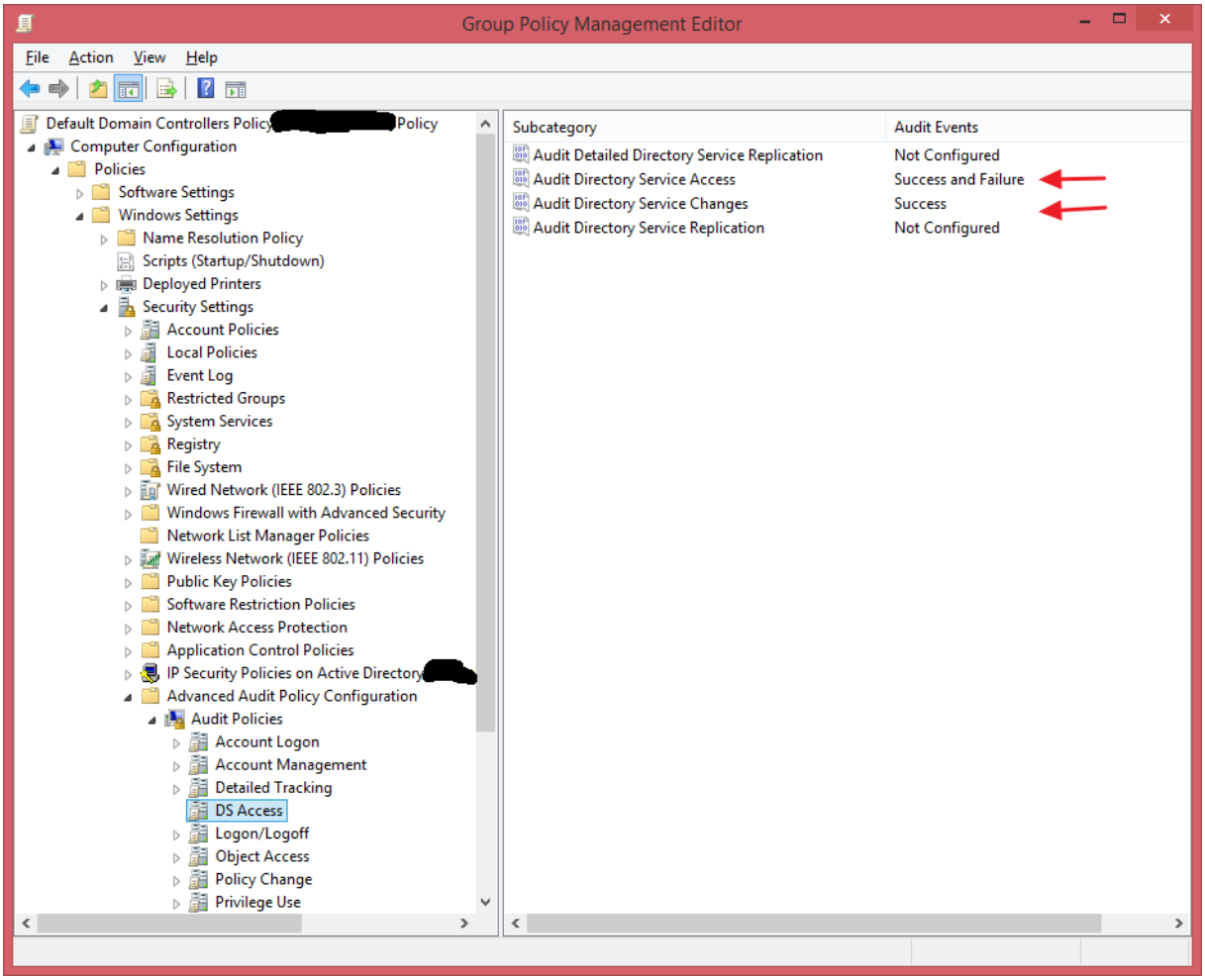
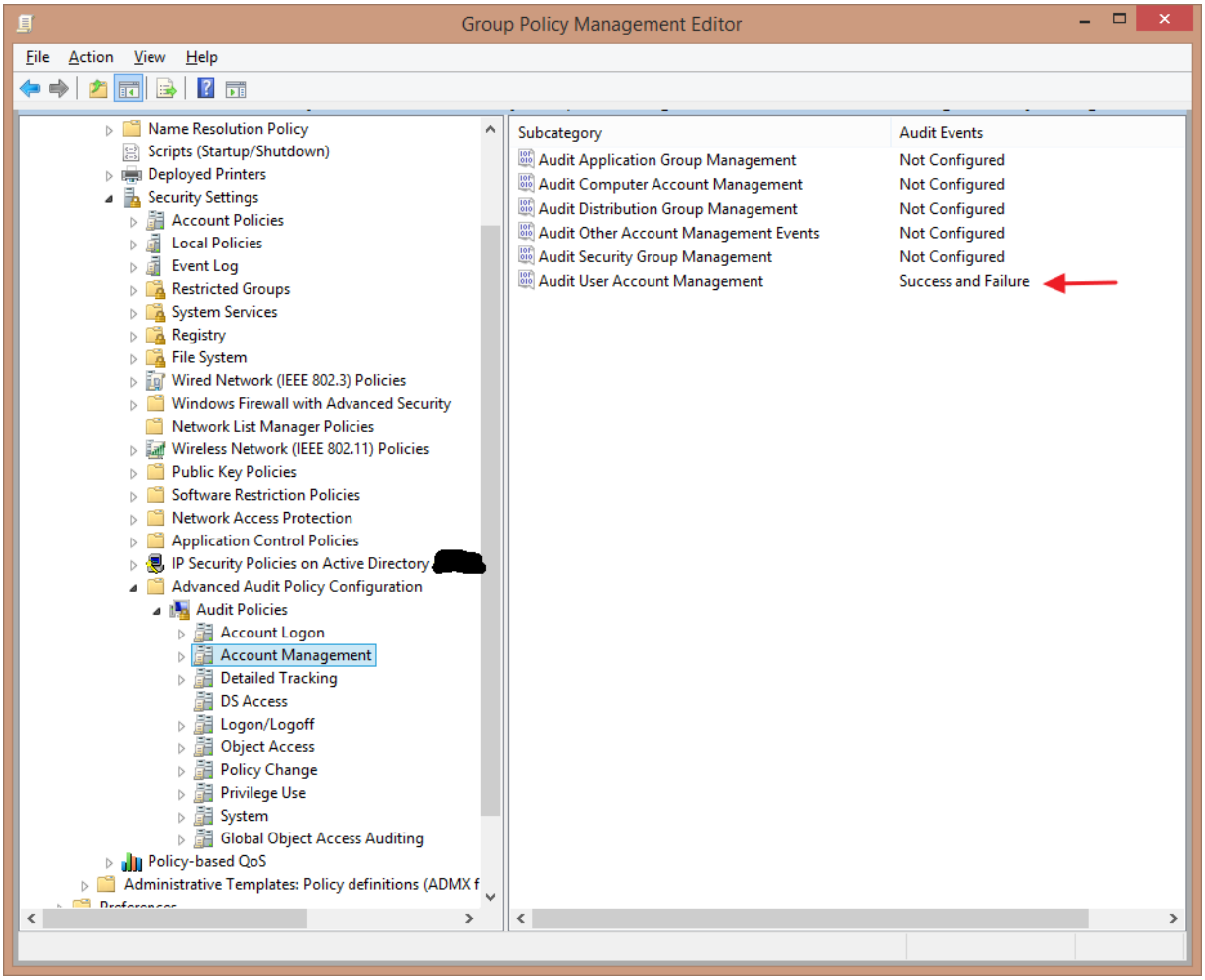
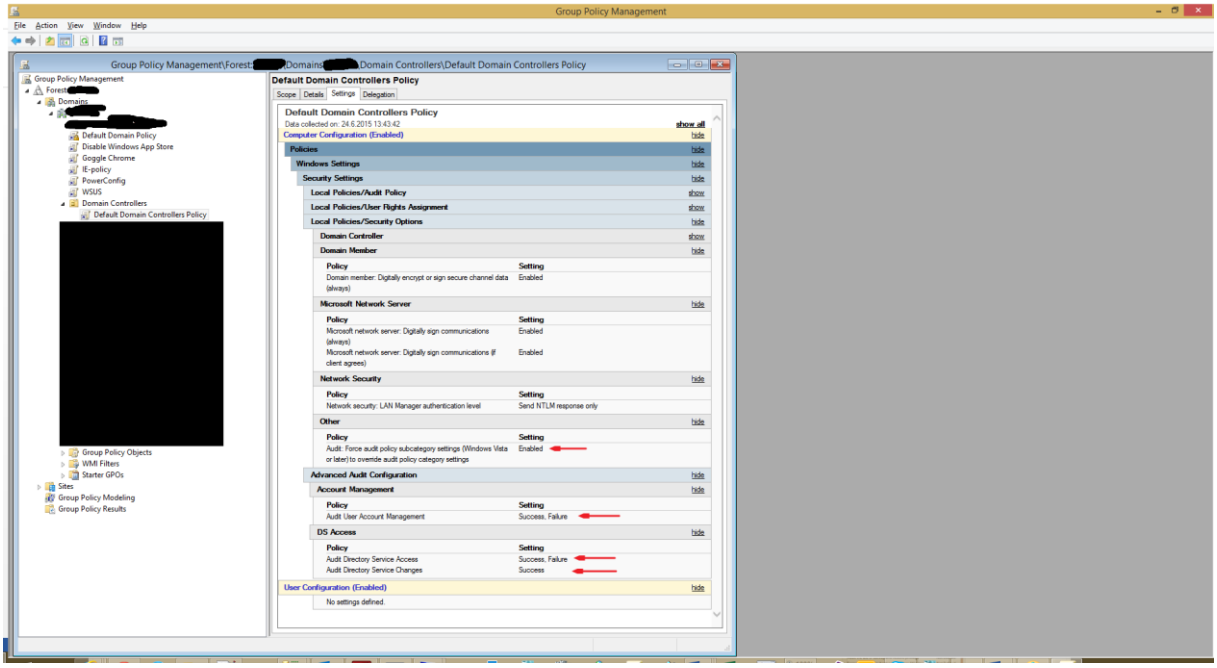
Active Directory change auditing screenshots

Note – these screenshots are from Windows Server 2012 R2.

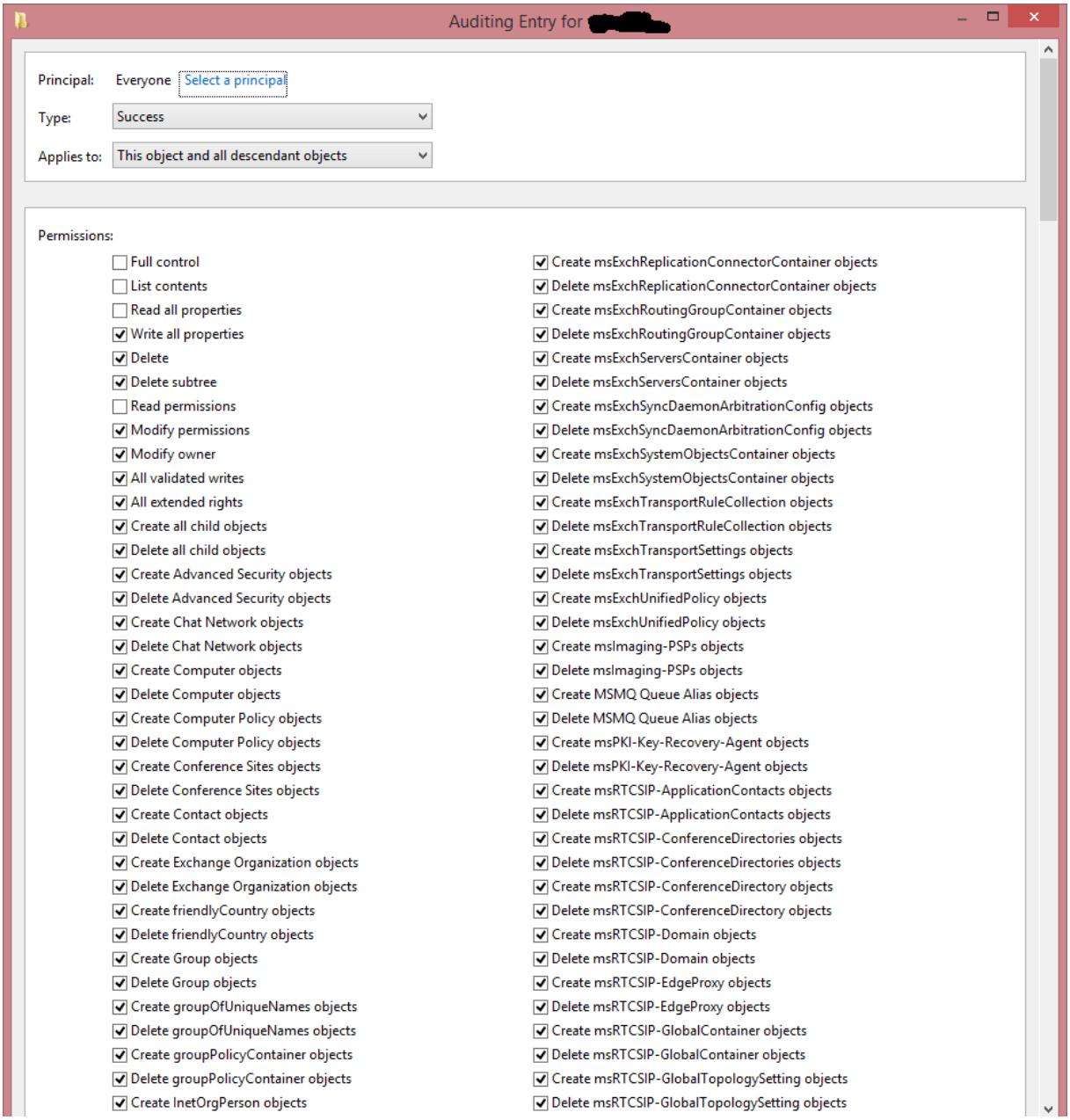


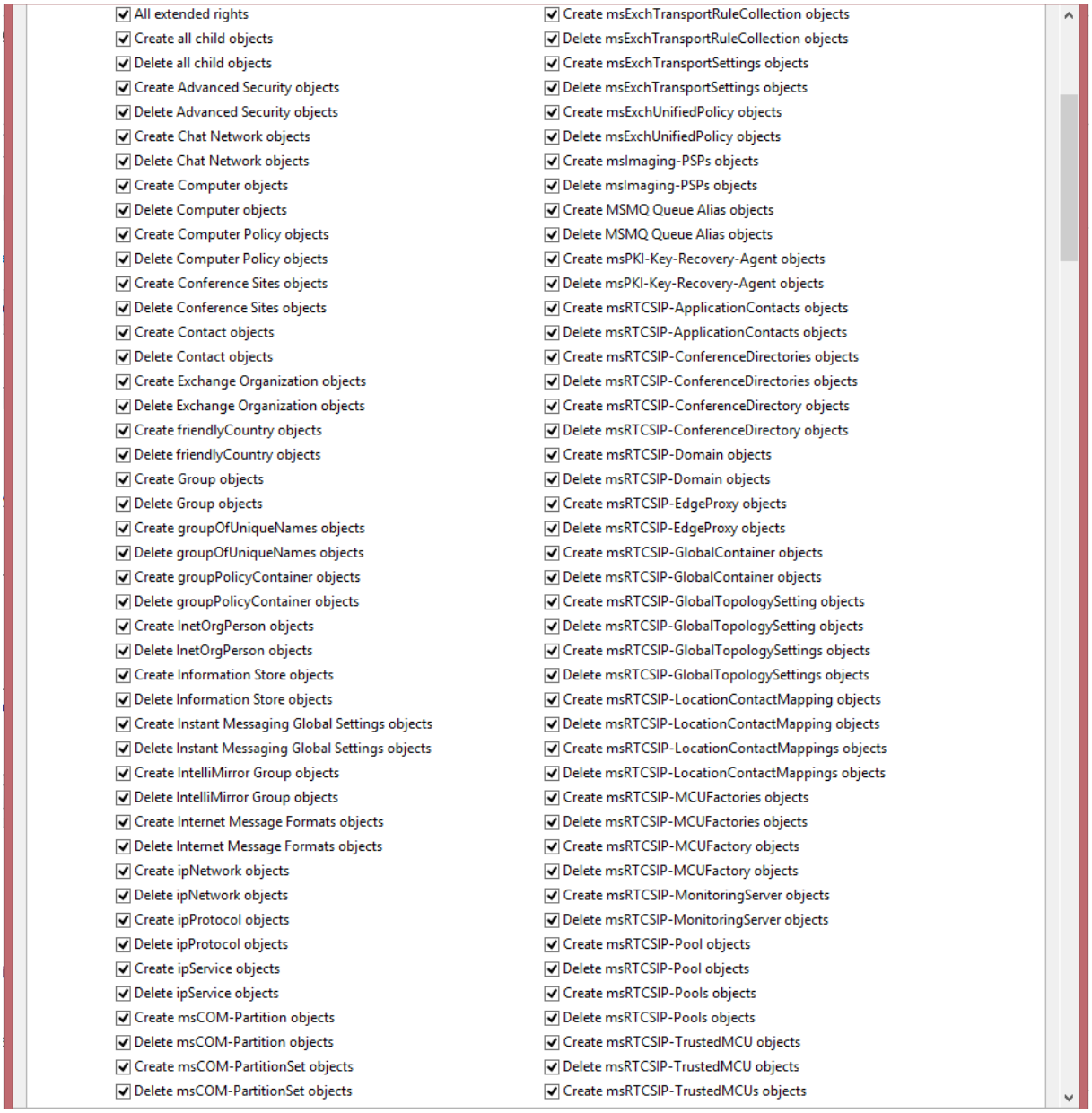


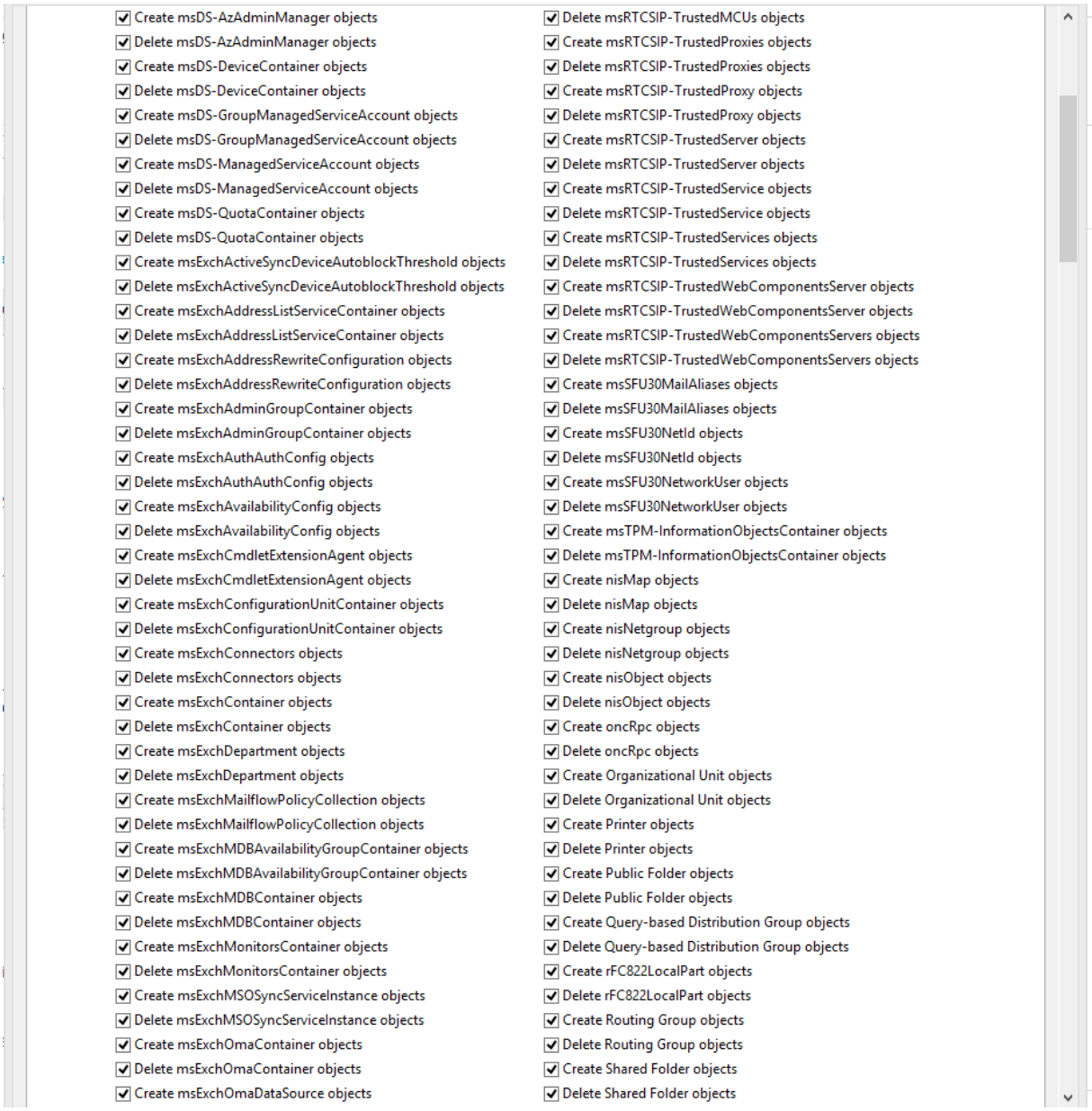

Group Policy Management Editor
File Action View Help
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS
Administrative Templates: Policy definitions (ADMX f
Subcategory
Audit Events
Audit Application Group Management
Not Configured
Audit Computer Account Management
Not Configured
Audit Distribution Group Management
Not Configured
Audit Other Account Management Events
Not Configured
Audit Security Group Management
Not Configured
Audit User Account Management
Success and Failure

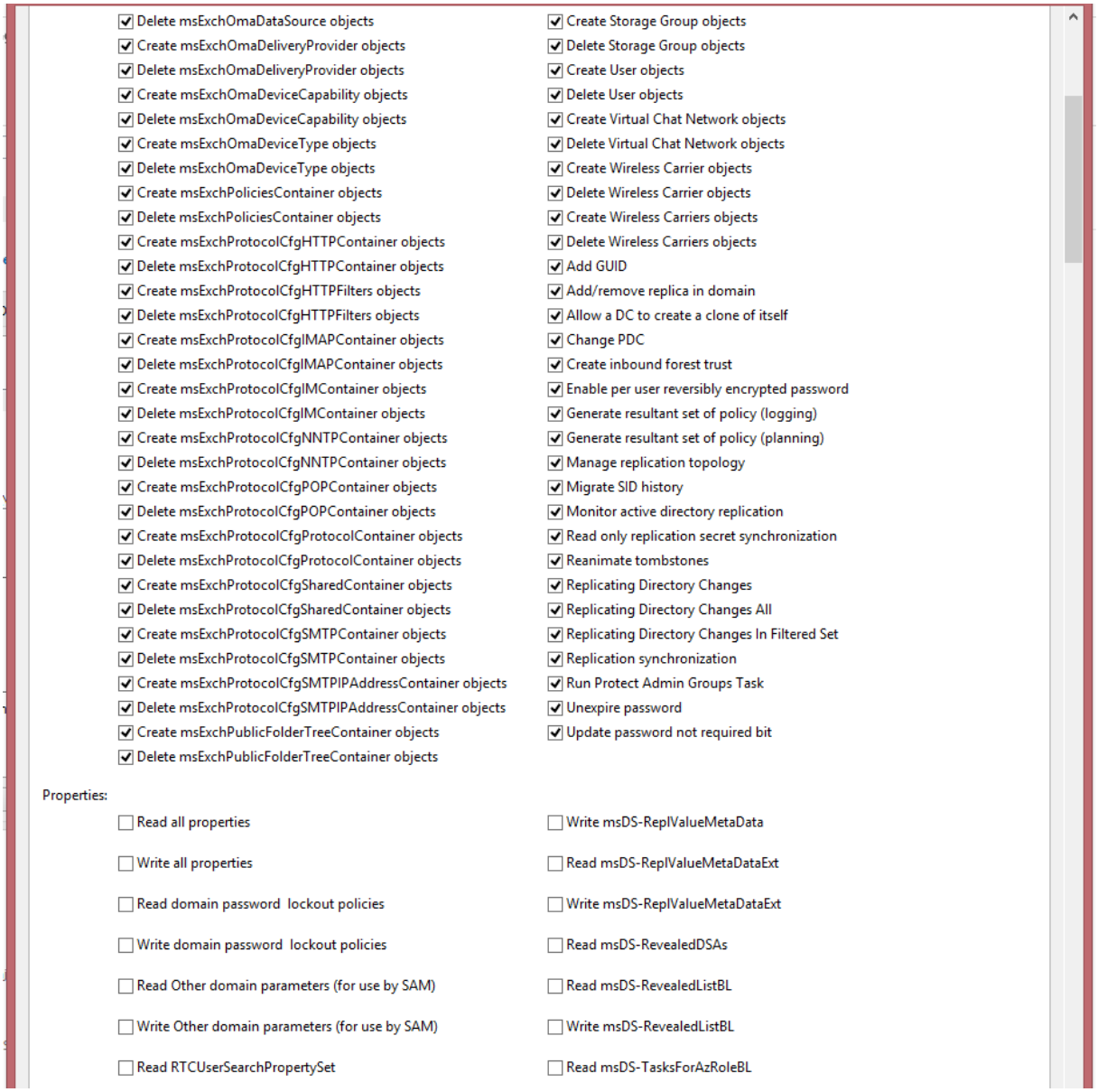

Group Policy Management
File Action View Window Help
Group Policy Management\Forest: [redacted]\Domains\[redacted]\Domain Controllers\Default Domain Controllers Policy
Default Domain Controllers Policy
Scope Details Settings Delegation
Default Domain Controllers Policy
Data collected on: 24.6.2015 13:43:42
show all
Computer Configuration (Enabled)
hide
Policies
Windows Settings
Security Settings
Local Policies/Audit Policy
Local Policies/User Rights Assignment
Local Policies/Security Options
Domain Controller
Domain Member
Policy
Setting
Domain member: Digitally encrypt or sign secure channel data (always)
Enabled
Microsoft Network Server
Microsoft network server: Digitally sign communications (always)
Microsoft network server: Digitally sign communications (if client agrees)
Network Security
Network security: LAN Manager authentication level
Send NTLM response only
Other
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings
Enabled
Advanced Audit Configuration
Account Management
Audit User Account Management
Success, Failure
DS Access
Audit Directory Service Access
Audit Directory Service Changes
Success, Failure
Success
User Configuration (Enabled)
No settings defined.

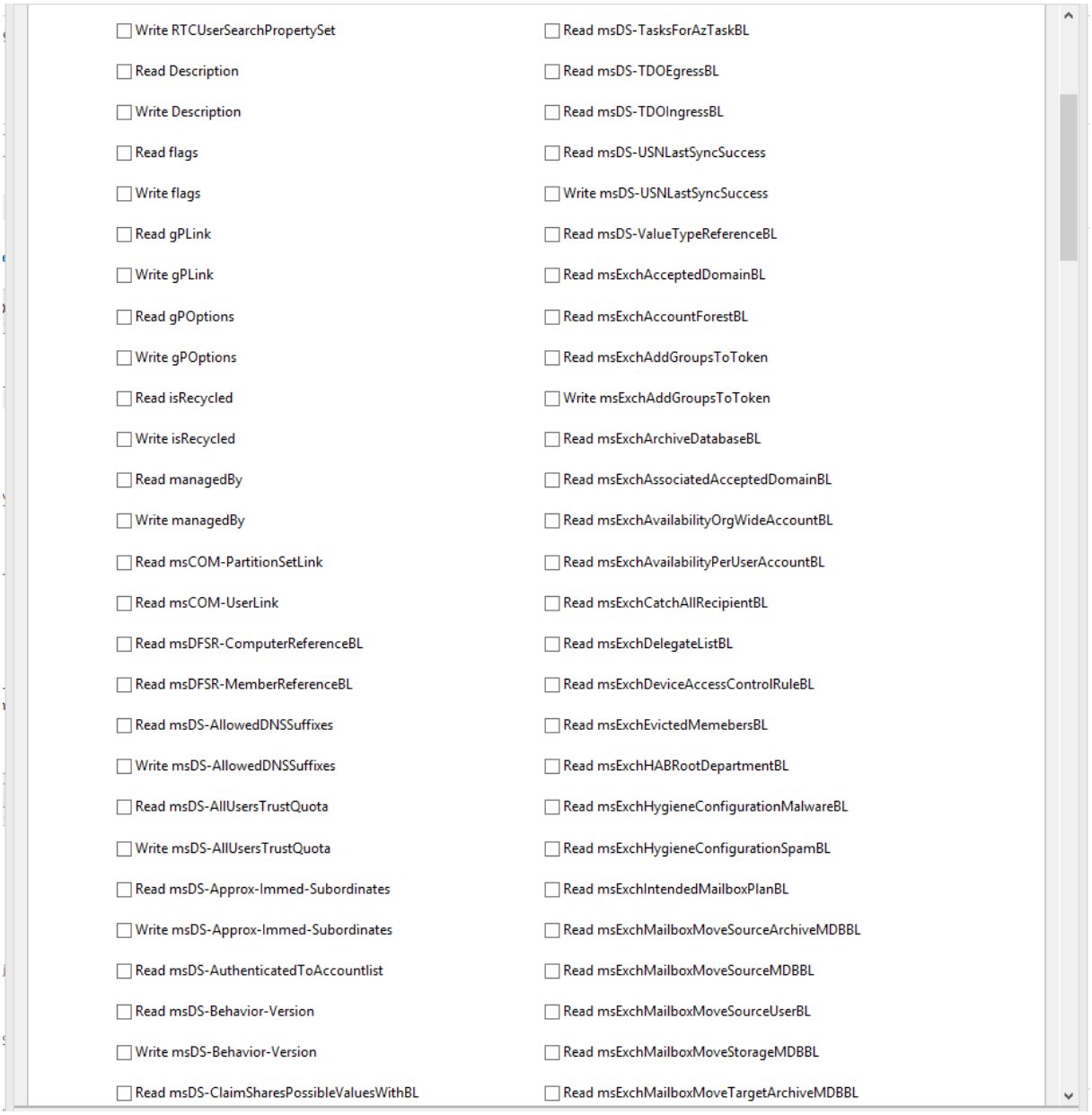
Right click on Domain name in Active Directory Users and Computers, select Properties, click on Advanced button, select Auditing tab, click on Add button, click „Select a principal“ link, type „Everyone“, click OK button, see following screenshots:

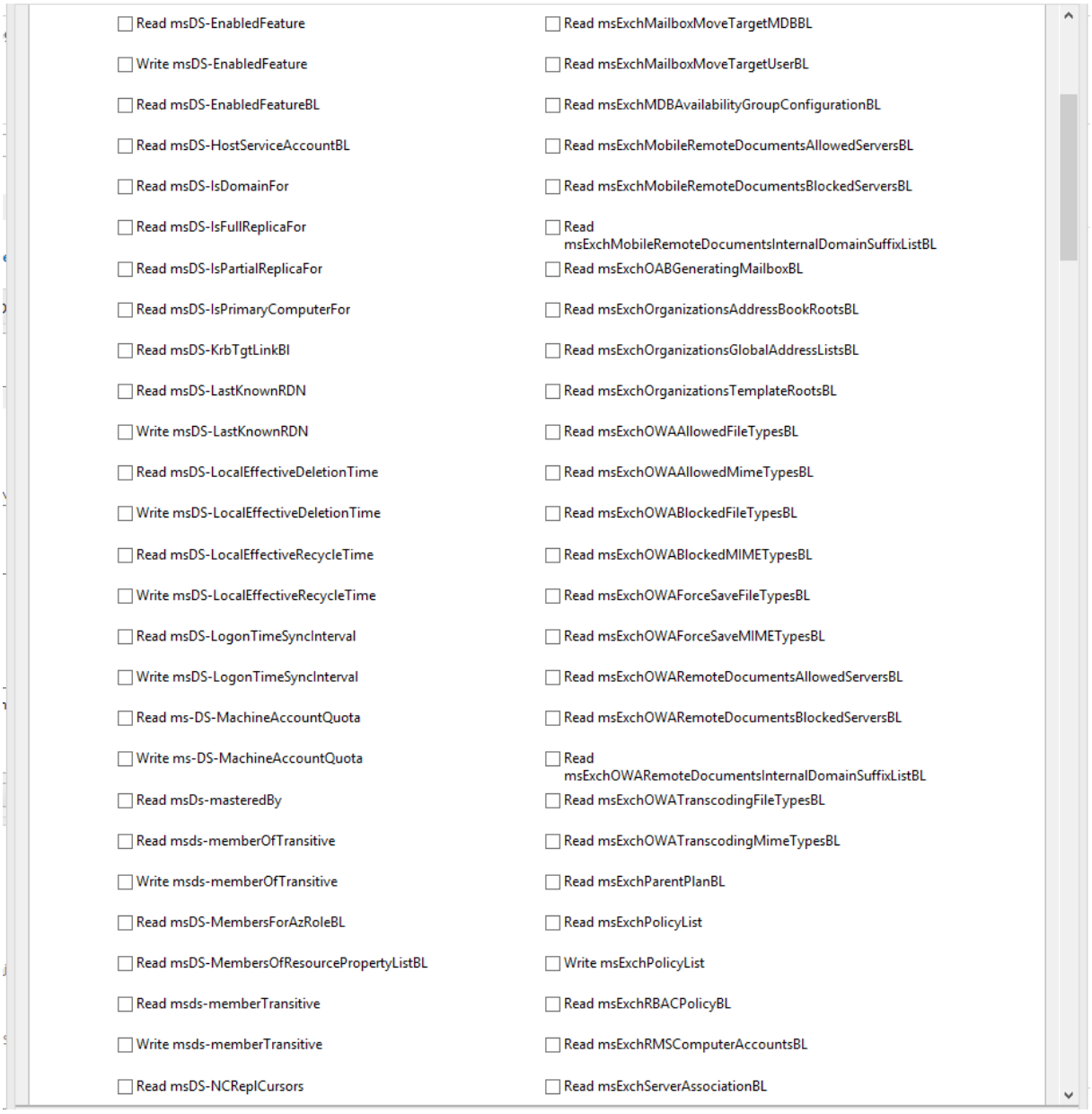


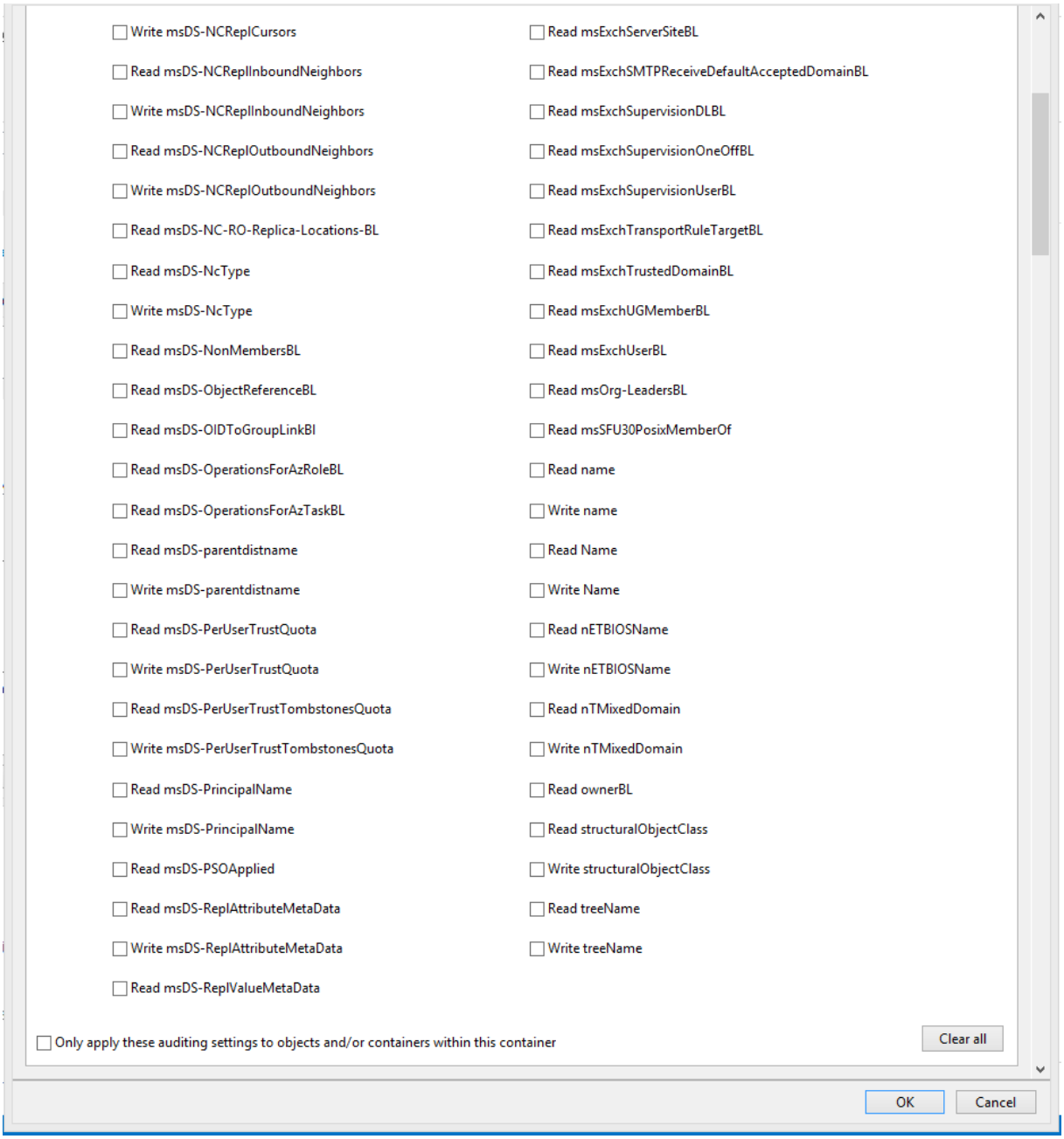

All extended rights
Create all child objects
Delete all child objects
Create Advanced Security objects
Delete Advanced Security objects
Create Chat Network objects
Delete Chat Network objects
Create Computer objects
Delete Computer objects
Create Computer Policy objects
Delete Computer Policy objects
Create Conference Sites objects
Delete Conference Sites objects
Create Contact objects
Delete Contact objects
Create Exchange Organization objects
Delete Exchange Organization objects
Create friendlyCountry objects
Delete friendlyCountry objects
Create Group objects
Delete Group objects
Create groupOfUniqueNames objects
Delete groupOfUniqueNames objects
Create groupPolicyContainer objects
Delete groupPolicyContainer objects
Create InetOrgPerson objects
Delete InetOrgPerson objects
Create Information Store objects
Delete Information Store objects
Create Instant Messaging Global Settings objects
Delete Instant Messaging Global Settings objects
Create IntelliMirror Group objects
Delete IntelliMirror Group objects
Create Internet Message Formats objects
Delete Internet Message Formats objects
Create ipNetwork objects
Delete ipNetwork objects
Create ipProtocol objects
Delete ipProtocol objects
Create ipService objects
Delete ipService objects
Create msCOM-Partition objects
Delete msCOM-Partition objects
Create msCOM-PartitionSet objects
Delete msCOM-PartitionSet objects
Create msExchTransportRuleCollection objects
Delete msExchTransportRuleCollection objects
Create msExchTransportSettings objects
Delete msExchTransportSettings objects
Create msExchUnifiedPolicy objects
Delete msExchUnifiedPolicy objects
Create msImaging-PSPs objects
Delete msImaging-PSPs objects
Create MSMQ Queue Alias objects
Delete MSMQ Queue Alias objects
Create msPKI-Key-Recovery-Agent objects
Delete msPKI-Key-Recovery-Agent objects
Create msRTCSIP-ApplicationContacts objects
Delete msRTCSIP-ApplicationContacts objects
Create msRTCSIP-ConferenceDirectories objects
Delete msRTCSIP-ConferenceDirectories objects
Create msRTCSIP-ConferenceDirectory objects
Delete msRTCSIP-ConferenceDirectory objects
Create msRTCSIP-Domain objects
Delete msRTCSIP-Domain objects
Create msRTCSIP-EdgeProxy objects
Delete msRTCSIP-EdgeProxy objects
Create msRTCSIP-GlobalContainer objects
Delete msRTCSIP-GlobalContainer objects
Create msRTCSIP-GlobalTopologySetting objects
Delete msRTCSIP-GlobalTopologySetting objects
Create msRTCSIP-GlobalTopologySettings objects
Delete msRTCSIP-GlobalTopologySettings objects
Create msRTCSIP-LocationContactMapping objects
Delete msRTCSIP-LocationContactMapping objects
Create msRTCSIP-LocationContactMappings objects
Delete msRTCSIP-LocationContactMappings objects
Create msRTCSIP-MCUFactories objects
Delete msRTCSIP-MCUFactories objects
Create msRTCSIP-MCUFactory objects
Delete msRTCSIP-MCUFactory objects
Create msRTCSIP-MonitoringServer objects
Delete msRTCSIP-MonitoringServer objects
Create msRTCSIP-Pool objects
Delete msRTCSIP-Pool objects
Create msRTCSIP-Pools objects
Delete msRTCSIP-Pools objects
Create msRTCSIP-TrustedMCU objects
Delete msRTCSIP-TrustedMCU objects
Create msRTCSIP-TrustedMCUs objects

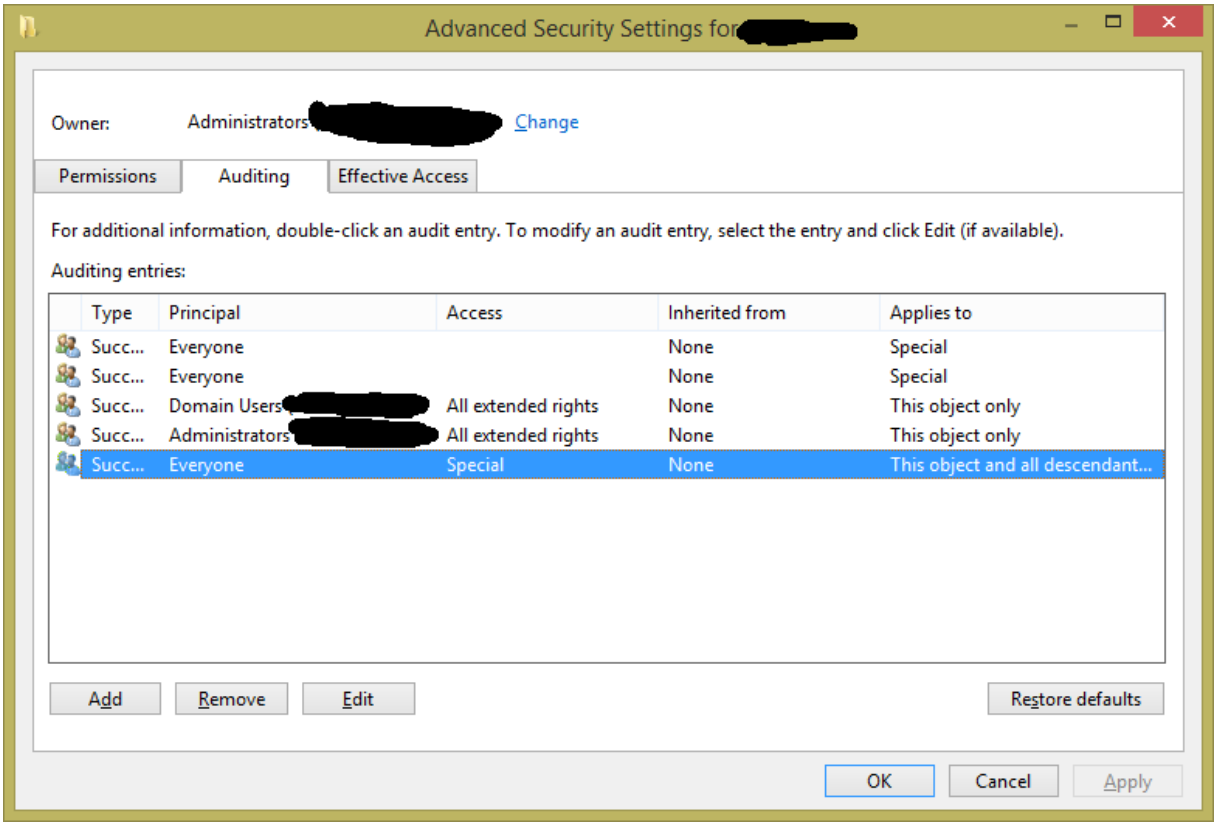

Create msDS-AzAdminManager objects
Delete msDS-AzAdminManager objects
Create msDS-DeviceContainer objects
Delete msDS-DeviceContainer objects
Create msDS-GroupManagedServiceAccount objects
Delete msDS-GroupManagedServiceAccount objects
Create msDS-ManagedServiceAccount objects
Delete msDS-ManagedServiceAccount objects
Create msDS-QuotaContainer objects
Delete msDS-QuotaContainer objects
Create msExchActiveSyncDeviceAutoblockThreshold objects
Delete msExchActiveSyncDeviceAutoblockThreshold objects
Create msExchAddressListServiceContainer objects
Delete msExchAddressListServiceContainer objects
Create msExchAddressRewriteConfiguration objects
Delete msExchAddressRewriteConfiguration objects
Create msExchAdminGroupContainer objects
Delete msExchAdminGroupContainer objects
Create msExchAuthAuthConfig objects
Delete msExchAuthAuthConfig objects
Create msExchAvailabilityConfig objects
Delete msExchAvailabilityConfig objects
Create msExchCmdletExtensionAgent objects
Delete msExchCmdletExtensionAgent objects
Create msExchConfigurationUnitContainer objects
Delete msExchConfigurationUnitContainer objects
Create msExchConnectors objects
Delete msExchConnectors objects
Create msExchContainer objects
Delete msExchContainer objects
Create msExchDepartment objects
Delete msExchDepartment objects
Create msExchMailflowPolicyCollection objects
Delete msExchMailflowPolicyCollection objects
Create msExchMDBAvailabilityGroupContainer objects
Delete msExchMDBAvailabilityGroupContainer objects
Create msExchMDBContainer objects
Delete msExchMDBContainer objects
Create msExchMonitorsContainer objects
Delete msExchMonitorsContainer objects
Create msExchMSOSyncServiceInstance objects
Delete msExchMSOSyncServiceInstance objects
Create msExchOmaContainer objects
Delete msExchOmaContainer objects
Create msExchOmaDataSource objects
Delete msRTCSIP-TrustedMCUs objects
Create msRTCSIP-TrustedProxies objects
Delete msRTCSIP-TrustedProxies objects
Create msRTCSIP-TrustedProxy objects
Delete msRTCSIP-TrustedProxy objects
Create msRTCSIP-TrustedServer objects
Delete msRTCSIP-TrustedServer objects
Create msRTCSIP-TrustedService objects
Delete msRTCSIP-TrustedService objects
Create msRTCSIP-TrustedServices objects
Delete msRTCSIP-TrustedServices objects
Create msRTCSIP-TrustedWebComponentsServer objects
Delete msRTCSIP-TrustedWebComponentsServer objects
Create msRTCSIP-TrustedWebComponentsServers objects
Delete msRTCSIP-TrustedWebComponentsServers objects
Create msSFU30MailAliases objects
Delete msSFU30MailAliases objects
Create msSFU30NetId objects
Delete msSFU30NetId objects
Create msSFU30NetworkUser objects
Delete msSFU30NetworkUser objects
Create msTPM-InformationObjectsContainer objects
Delete msTPM-InformationObjectsContainer objects
Create nisMap objects
Delete nisMap objects
Create nisNetgroup objects
Delete nisNetgroup objects
Create nisObject objects
Delete nisObject objects
Create oncRpc objects
Delete oncRpc objects
Create Organizational Unit objects
Delete Organizational Unit objects
Create Printer objects
Delete Printer objects
Create Public Folder objects
Delete Public Folder objects
Create Query-based Distribution Group objects
Delete Query-based Distribution Group objects
Create rFC822LocalPart objects
Delete rFC822LocalPart objects
Create Routing Group objects
Delete Routing Group objects
Create Shared Folder objects
Delete Shared Folder objects


Delete msExchOmaDataSource objects
Create msExchOmaDeliveryProvider objects
Delete msExchOmaDeliveryProvider objects
Create msExchOmaDeviceCapability objects
Delete msExchOmaDeviceCapability objects
Create msExchOmaDeviceType objects
Delete msExchOmaDeviceType objects
Create msExchPoliciesContainer objects
Delete msExchPoliciesContainer objects
Create msExchProtocolCfgHTTPContainer objects
Delete msExchProtocolCfgHTTPContainer objects
Create msExchProtocolCfgHTTPFilters objects
Delete msExchProtocolCfgHTTPFilters objects
Create msExchProtocolCfgIMAPContainer objects
Delete msExchProtocolCfgIMAPContainer objects
Create msExchProtocolCfgIMContainer objects
Delete msExchProtocolCfgIMContainer objects
Create msExchProtocolCfgNNTPContainer objects
Delete msExchProtocolCfgNNTPContainer objects
Create msExchProtocolCfgPOPContainer objects
Delete msExchProtocolCfgPOPContainer objects
Create msExchProtocolCfgProtocolContainer objects
Delete msExchProtocolCfgProtocolContainer objects
Create msExchProtocolCfgSharedContainer objects
Delete msExchProtocolCfgSharedContainer objects
Create msExchProtocolCfgSMTPContainer objects
Delete msExchProtocolCfgSMTPContainer objects
Create msExchProtocolCfgSMTPIPAddressContainer objects
Delete msExchProtocolCfgSMTPIPAddressContainer objects
Create msExchPublicFolderTreeContainer objects
Delete msExchPublicFolderTreeContainer objects
Create Storage Group objects
Delete Storage Group objects
Create User objects
Delete User objects
Create Virtual Chat Network objects
Delete Virtual Chat Network objects
Create Wireless Carrier objects
Delete Wireless Carrier objects
Create Wireless Carriers objects
Delete Wireless Carriers objects
Add GUID
Add/remove replica in domain
Allow a DC to create a clone of itself
Change PDC
Create inbound forest trust
Enable per user reversibly encrypted password
Generate resultant set of policy (logging)
Generate resultant set of policy (planning)
Manage replication topology
Migrate SID history
Monitor active directory replication
Read only replication secret synchronization
Reanimate tombstones
Replicating Directory Changes
Replicating Directory Changes All
Replicating Directory Changes In Filtered Set
Replication synchronization
Run Protect Admin Groups Task
Unexpire password
Update password not required bit
Properties:
Read all properties
Write all properties
Read domain password lockout policies
Write domain password lockout policies
Read Other domain parameters (for use by SAM)
Write Other domain parameters (for use by SAM)
Read RTCUserSearchPropertySet
Write msDS-ReplValueMetaData
Read msDS-ReplValueMetaDataExt
Write msDS-ReplValueMetaDataExt
Read msDS-RevealedDSAs
Read msDS-RevealedListBL
Write msDS-RevealedListBL
Read msDS-TasksForAzRoleBL


Write RTCUserSearchPropertySet
Read Description
Write Description
Read flags
Write flags
Read gPLink
Write gPLink
Read gPOptions
Write gPOptions
Read isRecycled
Write isRecycled
Read managedBy
Write managedBy
Read msCOM-PartitionSetLink
Read msCOM-UserLink
Read msDFSR-ComputerReferenceBL
Read msDFSR-MemberReferenceBL
Read msDS-AllowedDNSSuffixes
Write msDS-AllowedDNSSuffixes
Read msDS-AllUsersTrustQuota
Write msDS-AllUsersTrustQuota
Read msDS-Approx-Immed-Subordinates
Write msDS-Approx-Immed-Subordinates
Read msDS-AuthenticatedToAccountlist
Read msDS-Behavior-Version
Write msDS-Behavior-Version
Read msDS-ClaimSharesPossibleValuesWithBL
Read msDS-TasksForAzTaskBL
Read msDS-TDOEgressBL
Read msDS-TDOIngressBL
Read msDS-USNLastSyncSuccess
Write msDS-USNLastSyncSuccess
Read msDS-ValueTypeReferenceBL
Read msExchAcceptedDomainBL
Read msExchAccountForestBL
Read msExchAddGroupsToToken
Write msExchAddGroupsToToken
Read msExchArchiveDatabaseBL
Read msExchAssociatedAcceptedDomainBL
Read msExchAvailabilityOrgWideAccountBL
Read msExchAvailabilityPerUserAccountBL
Read msExchCatchAllRecipientBL
Read msExchDelegateListBL
Read msExchDeviceAccessControlRuleBL
Read msExchEvictedMemebersBL
Read msExchHABRootDepartmentBL
Read msExchHygieneConfigurationMalwareBL
Read msExchHygieneConfigurationSpamBL
Read msExchIntendedMailboxPlanBL
Read msExchMailboxMoveSourceArchiveMDBBL
Read msExchMailboxMoveSourceMDBBL
Read msExchMailboxMoveSourceUserBL
Read msExchMailboxMoveStorageMDBBL
Read msExchMailboxMoveTargetArchiveMDBBL


Read msDS-EnabledFeature
Write msDS-EnabledFeature
Read msDS-EnabledFeatureBL
Read msDS-HostServiceAccountBL
Read msDS-IsDomainFor
Read msDS-IsFullReplicaFor
Read msDS-IsPartialReplicaFor
Read msDS-IsPrimaryComputerFor
Read msDS-KrbTgtLinkBl
Read msDS-LastKnownRDN
Write msDS-LastKnownRDN
Read msDS-LocalEffectiveDeletionTime
Write msDS-LocalEffectiveDeletionTime
Read msDS-LocalEffectiveRecycleTime
Write msDS-LocalEffectiveRecycleTime
Read msDS-LogonTimeSyncInterval
Write msDS-LogonTimeSyncInterval
Read ms-DS-MachineAccountQuota
Write ms-DS-MachineAccountQuota
Read msDs-masteredBy
Read msds-memberOfTransitive
Write msds-memberOfTransitive
Read msDS-MembersForAzRoleBL
Read msDS-MembersOfResourcePropertyListBL
Read msds-memberTransitive
Write msds-memberTransitive
Read msDS-NCReplCursors
Read msExchMailboxMoveTargetMDBBL
Read msExchMailboxMoveTargetUserBL
Read msExchMDBAvailabilityGroupConfigurationBL
Read msExchMobileRemoteDocumentsAllowedServersBL
Read msExchMobileRemoteDocumentsBlockedServersBL
Read msExchMobileRemoteDocumentsInternalDomainSuffixListBL
Read msExchOABGeneratingMailboxBL
Read msExchOrganizationsAddressBookRootsBL
Read msExchOrganizationsGlobalAddressListsBL
Read msExchOrganizationsTemplateRootsBL
Read msExchOWAAllowedFileTypesBL
Read msExchOWAAllowedMimeTypesBL
Read msExchOWABlockedFileTypesBL
Read msExchOWABlockedMIMETypesBL
Read msExchOWAForceSaveFileTypesBL
Read msExchOWAForceSaveMIMETypesBL
Read msExchOWARemoteDocumentsAllowedServersBL
Read msExchOWARemoteDocumentsBlockedServersBL
Read msExchOWARemoteDocumentsInternalDomainSuffixListBL
Read msExchOWATranscodingFileTypesBL
Read msExchOWATranscodingMimeTypesBL
Read msExchParentPlanBL
Read msExchPolicyList
Write msExchPolicyList
Read msExchRBACPolicyBL
Read msExchRMSComputerAccountsBL
Read msExchServerAssociationBL


Write msDS-NCReplCursors
Read msDS-NCReplInboundNeighbors
Write msDS-NCReplInboundNeighbors
Read msDS-NCReplOutboundNeighbors
Write msDS-NCReplOutboundNeighbors
Read msDS-NC-RO-Replica-Locations-BL
Read msDS-NcType
Write msDS-NcType
Read msDS-NonMembersBL
Read msDS-ObjectReferenceBL
Read msDS-OIDToGroupLinkBl
Read msDS-OperationsForAzRoleBL
Read msDS-OperationsForAzTaskBL
Read msDS-parentdistname
Write msDS-parentdistname
Read msDS-PerUserTrustQuota
Write msDS-PerUserTrustQuota
Read msDS-PerUserTrustTombstonesQuota
Write msDS-PerUserTrustTombstonesQuota
Read msDS-PrincipalName
Write msDS-PrincipalName
Read msDS-PSOApplied
Read msDS-ReplAttributeMetaData
Write msDS-ReplAttributeMetaData
Read msDS-ReplValueMetaData
Read msExchServerSiteBL
Read msExchSMTPReceiveDefaultAcceptedDomainBL
Read msExchSupervisionDLBL
Read msExchSupervisionOneOffBL
Read msExchSupervisionUserBL
Read msExchTransportRuleTargetBL
Read msExchTrustedDomainBL
Read msExchUGMemberBL
Read msExchUserBL
Read msOrg-LeadersBL
Read msSFU30PosixMemberOf
Read name
Write name
Read Name
Write Name
Read nETBIOSName
Write nETBIOSName
Read nTMixedDomain
Write nTMixedDomain
Read ownerBL
Read structuralObjectClass
Write structuralObjectClass
Read treeName
Write treeName
Only apply these auditing settings to objects and/or containers within this container
Clear all
OK
Cancel


Advanced Security Settings for [redacted]
Owner: Administrators [redacted] Change
Permissions
Auditing
Effective Access
For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).
Auditing entries:
Type
Principal
Access
Inherited from
Applies to
Succ... Everyone None Special
Succ... Everyone None Special
Succ... Domain Users [redacted] All extended rights None This object only
Succ... Administrators [redacted] All extended rights None This object only
Succ... Everyone Special None This object and all descendant...
Add
Remove
Edit
Restore defaults
OK
Cancel
Apply