Configuring managed device services in Group Policy

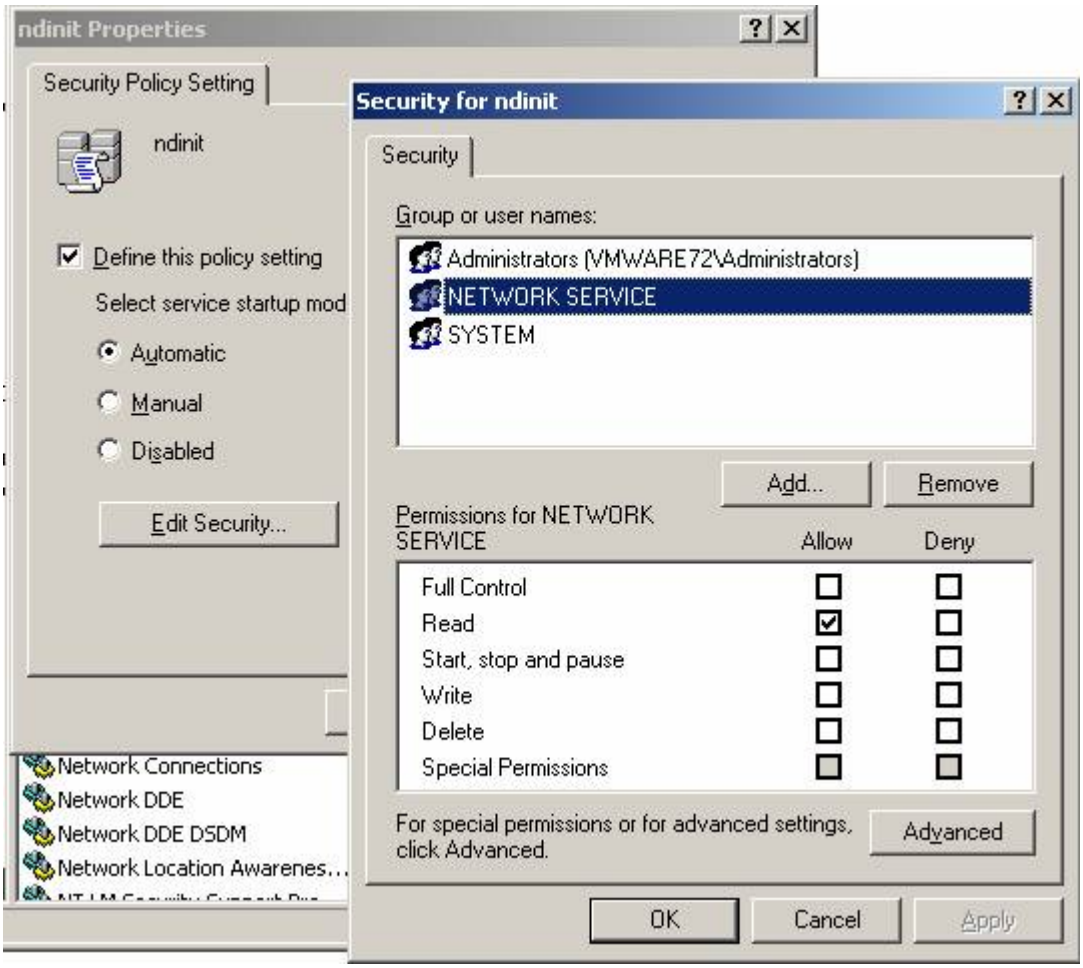
(Knowledge Base Article 100750)

This article describes how to configure the security settings for managed device services in Group Policy.

Service security configuration in Group Policy

The "ManageSoft managed device" (ndinit) service is a core component of the managed device scheduling infrastructure. Among other things, it keeps track of the currently running SYSTEM instance of the ManageSoft task scheduler process (ndtask). If you have configured ndinit service behavior using Group Policy, additional configuration is required to support managed devices running Windows XP SP2.

When you configure the ndinit service using Group Policy, the default security access control list (ACL) gives Full Control to SYSTEM and Administrators only. In XP SP1 and earlier, this is sufficient. However in SP2, a change to the DCOM inter-process communication mechanism means that the NETWORK SERVICE user now needs read access to the ndinit service. The following dialog shows how to add this user to the ACL in the ndinit service security settings in Group Policy:



Service configuration outside Group Policy

The default ACL for a service not configured through Group Policy gives read access to All Users, so no extra configuration is required if you are not configuring services via Group Policy.

More details on changes in Windows XP SP2

More information on this change in SP2 is available from Microsoft at
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx#EXDAC

"In Windows XP SP2, RPCSS is a key service for the RPC Endpoint Mapper and DCOM infrastructure. This service ran as Local System in previous versions of Windows. To reduce the attack surface of Windows and provide defense in depth, the RPCSS service functionality was split into two services. The RPCSS service with all the original functionality that did not require Local System privileges now runs under the Network Service account. A new DCOMLaunch service that includes functionality that requires Local System privileges runs under the Local System account."