RDP Session IDLE TIME

Das Ziel ist die Umsetzung einer **PCI** Anforderung zur **Härtung** von Servern. Die Anforderung besteht darin, das Zeitlimit für aktive RDP Sitzungen und das Leelaufsitzungslimit einzustellen.

Das Zeitlimit gibt die maximale Sitzungsdauer an, bevor die aktive Sitzung automatisch getrennt wird.

Das Leelaufsitzungslimit gibt an, wie lange die Verbindung ohne Benutzereingabe erhalten bleibt.

Das Ganze setzen wir mittels einer neuen **Gruppenrichtlinie** namens **Hardening RDP IDLE TIME** um.

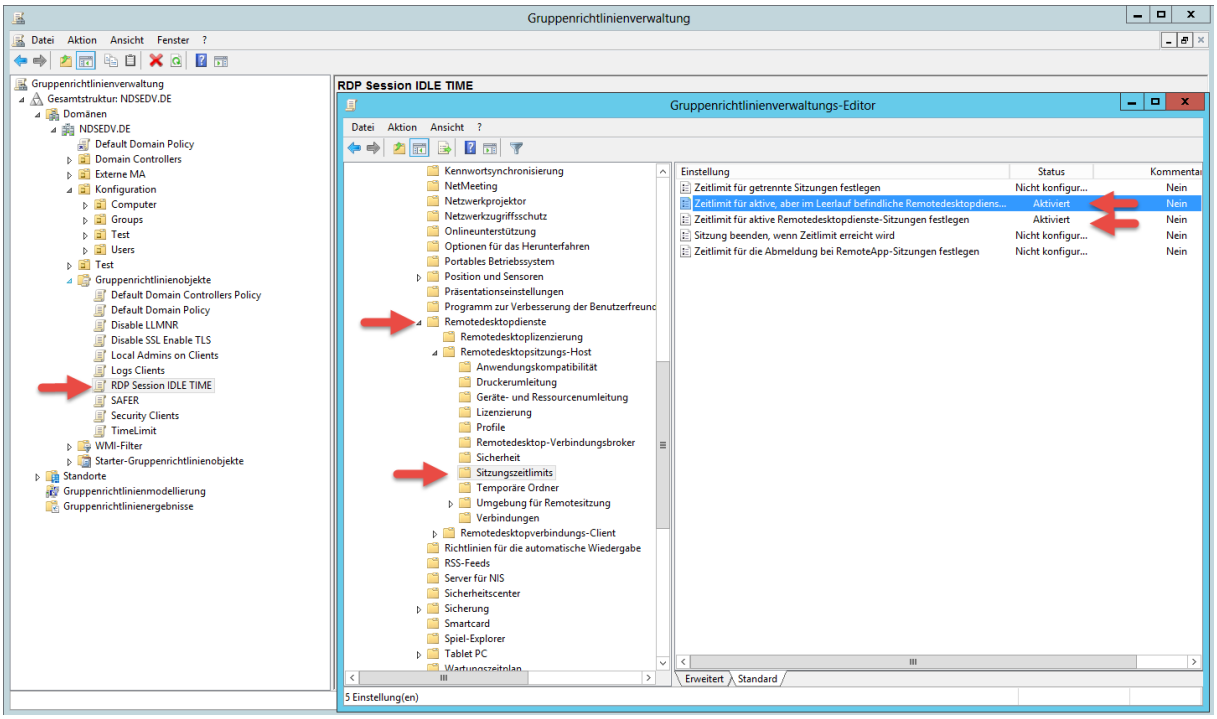
Dazu navigieren wir über **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Sessions Host > Session Time Limits** zu

- Set time limit for active Remote Desktop Services session und
- Set time limit for active but idle Remote Desktop Services sessions

German:

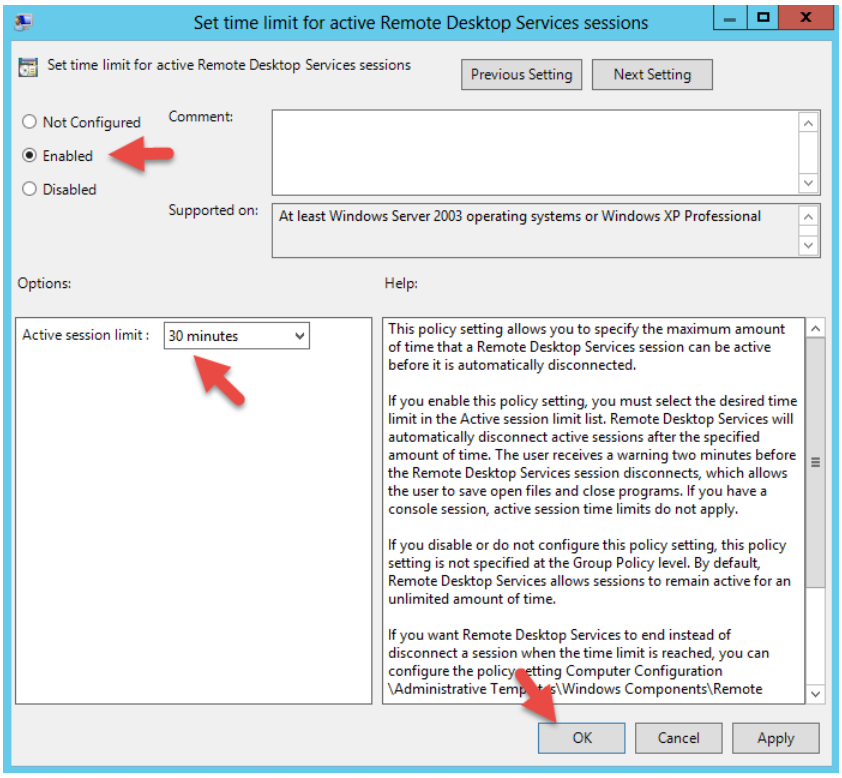
Dazu navigieren wir über **Computerkonfiguration > Administrative Vorlagen > Windowskomponenten > Remotedesktopdienste > Remotedesktopsitzungs-Host > Sitzungszeitlimit**

- Zeitlimit für aktive Remotedesktopdienste-Sitzung festlegen
- Zeitlimit für aktive, aber im Leerlauf befindliche Remotedesktopdienste-Sitzungen festlegen

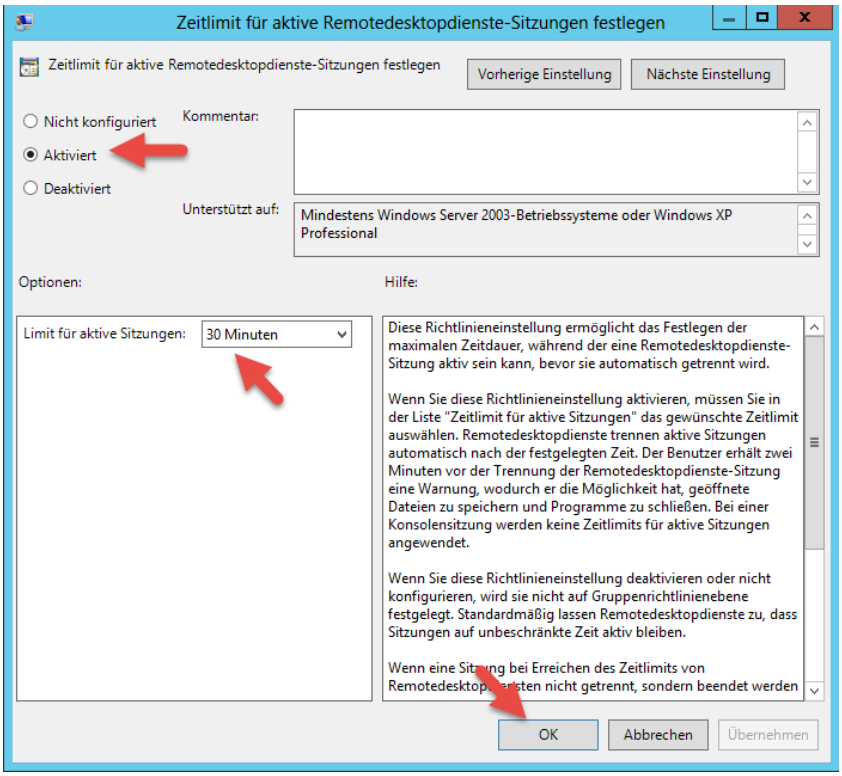


RDP Session IDLE TIME

Zur Umsetzung von "Set time limit for active Remote Desktop Services session" setze ich die Vorlage auf Enabled und einen Active Session Wert von 30 Minuten.

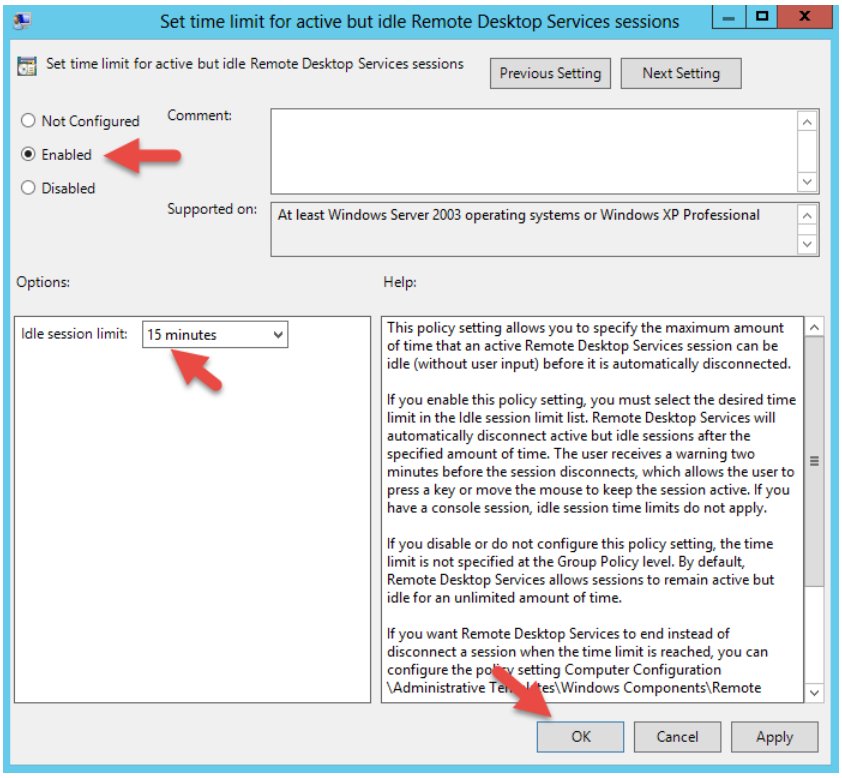


German:

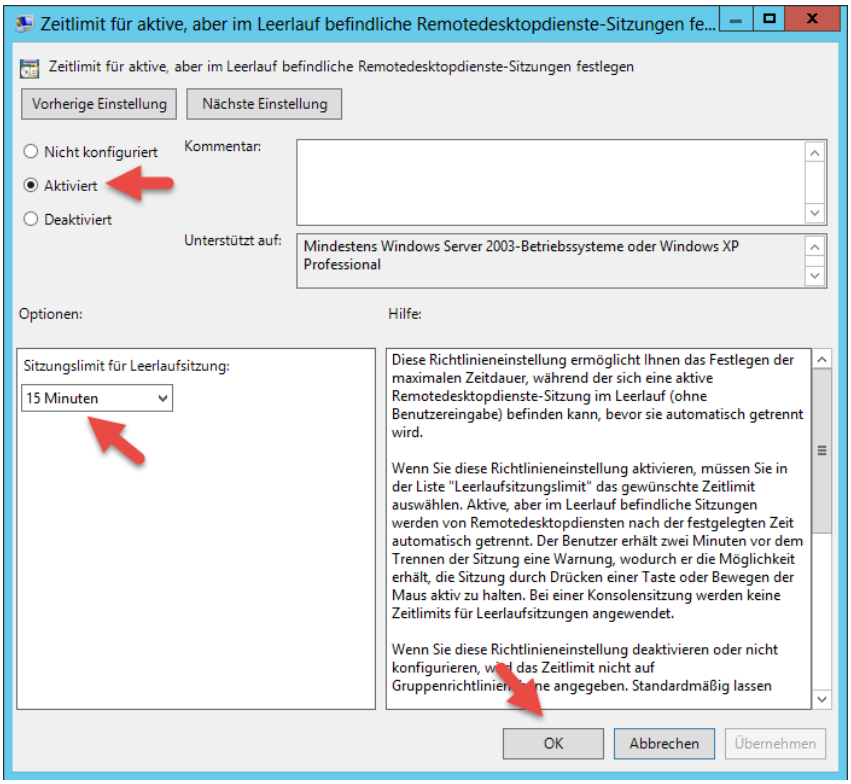


RDP Session IDLE TIME

Zur Umsetzung von "Set time limit for active but idle Remote Desktop Services sessions" setze ich die Vorlage auf Enabled und einen Idle session limit Wert von 15 Minuten.



German:



RDP Session IDLE TIME

GPO Bericht:

RDP Session IDLE TIME

Daten ermittelt am: 30.01.2016 17:14:39 — hide all

Allgemein — hide

Details — hide

Domäne	NDSEDV.DE
Besitzer	NDSEDV\Domänen-Admins
Erstellt	30.01.2016 17:01:02
Geändert	30.01.2016 17:04:50
Benutzerrevisionen	0 (AD), 0 (SYSVOL)
Computerrevisionen	3 (AD), 3 (SYSVOL)
Eindeutige ID	{8220C46F-D11E-4D5E-90B0-AEF1D644D741}
GPO-Status	Aktiviert

Verknüpfungen — hide

Standort	Erzwungen	Verknüpfungsstatus	Pfad
Keine			

Die Liste enthält Verknüpfungen zur Domäne des Gruppenrichtlinienobjekts.

Sicherheitsfilterung — hide

Die Einstellungen dieses Gruppenrichtlinienobjekts können nur auf folgenden Gruppen, Benutzer und Computer angewendet werden:

Name
NT-AUTORITÄT\Authentifizierte Benutzer

Delegierung — hide

Folgende Gruppen und Benutzer haben die angegebene Berechtigung für das Gruppenrichtlinienobjekt

Name	Zulässige Berechtigungen	Geerbt
NDSEDV\Domänen-Admins	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
NDSEDV\Organisations-Admins	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
NT-AUTORITÄT\Authentifizierte Benutzer	Lesen (durch Sicherheitsfilterung)	Nein
NT-AUTORITÄT\DOMÄNENCONTROLLER DER ORGANISATION	Lesen	Nein
NT-AUTORITÄT\SYSTEM	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein

Computerkonfiguration (Aktiviert) — hide

Richtlinien — hide

Administrative Vorlagen — hide

Richtliniendefinitionen (ADMX-Dateien) wurden beim lokalen Computer abgerufen.

Windows-Komponenten/Remotedesktopdienste/Remotedesktopsitzungs-Host/Sitzungszeitlimits — hide

Richtlinie	Einstellung	Kommentar
Zeitlimit für aktive Remotedesktopdienste-Sitzungen festlegen	Aktiviert	
Limit für aktive Sitzungen:	30 Minuten	

Richtlinie	Einstellung	Kommentar
Zeitlimit für aktive, aber im Leerlauf befindliche Remotedesktopdienste-Sitzungen festlegen	Aktiviert	
Sitzungslimit für Leerlaufsitzung:	15 Minuten	

Benutzerkonfiguration (Aktiviert) — hide

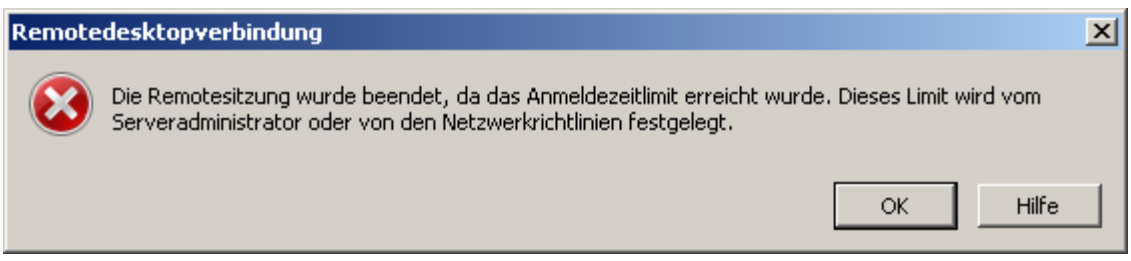
Keine Einstellungen definiert

Die neue Gruppenrichtlinie wird z.B. auf die **OU= > Server** verknüpft.

IDLE TIME Benachrichtigung:

Nach einer IDLE TIME von 13 Minuten kommt der erste Hinweis:

Nach weiteren 2 Minuten wird die Verbindung mit folgendem Hinweis getrennt:



RDP Session IDLE TIME

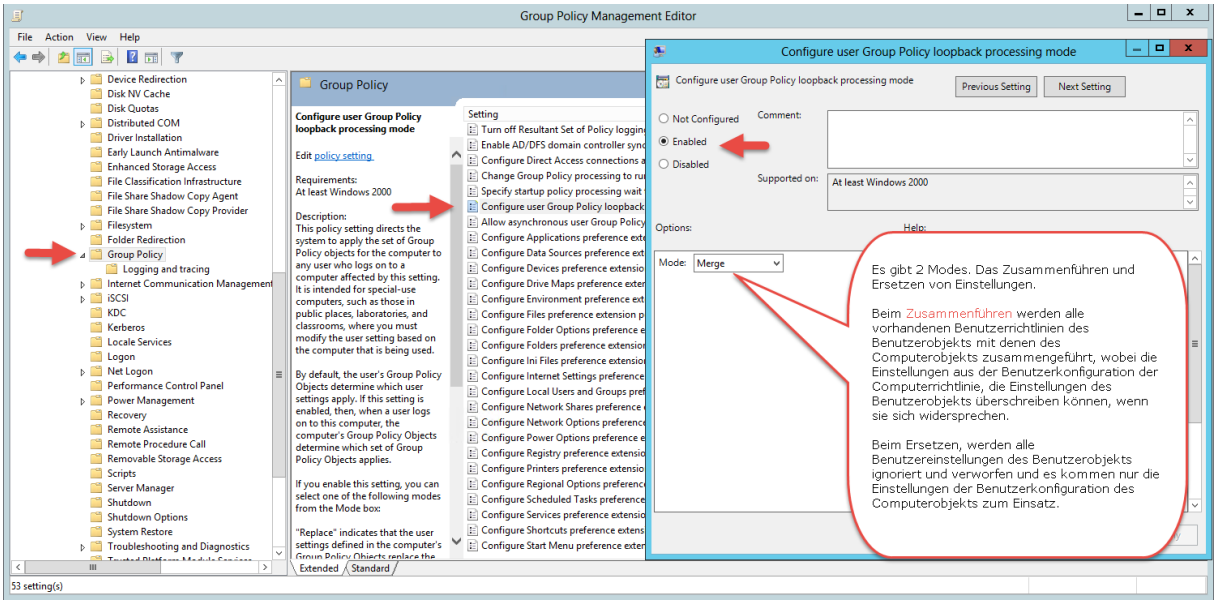
Alternative:

Statt die Session nach 15 Minuten IDLE TIME zu trennen erhöhen wir diese auf 30 Minuten und aktivieren dafür den Bildschirmschoner nach 15 Minuten Leerlaufzeit mit Kennwortabfrage.

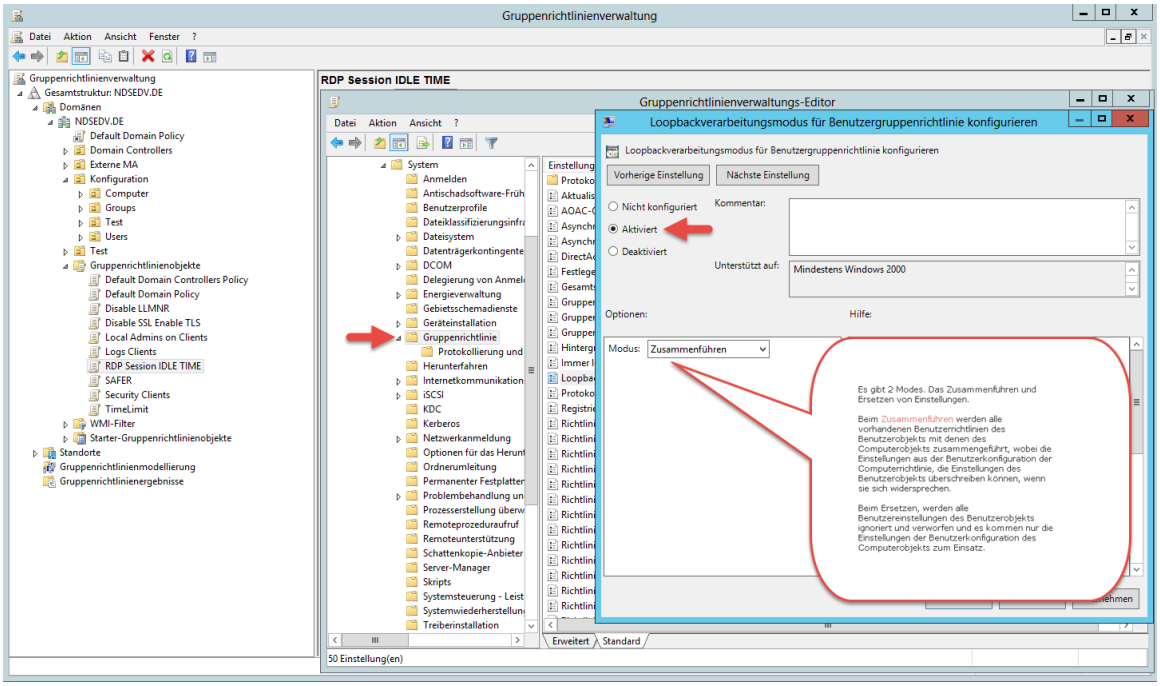
Die Änderungen an der Gruppenrichtlinie sehen wie folgt aus und umfassen weitere Einstellungen damit diese überhaupt verarbeitet werden kann.

Damit eine Computerrichtlinie einen konfigurierten benutzerspezifischen Teil verarbeiten kann, muss eine Loopbackverarbeitung eingerichtet werden. Dieser Loop erlaubt der Computerobjektbezogenen Richtlinie, die Verarbeitung des benutzerspezifischen konfigurierten Teils dieser Richtlinie, da sie ansonsten keine Berücksichtigung finden würde. Sollte allen klar sein.

Loopback Verarbeitung aktivieren:

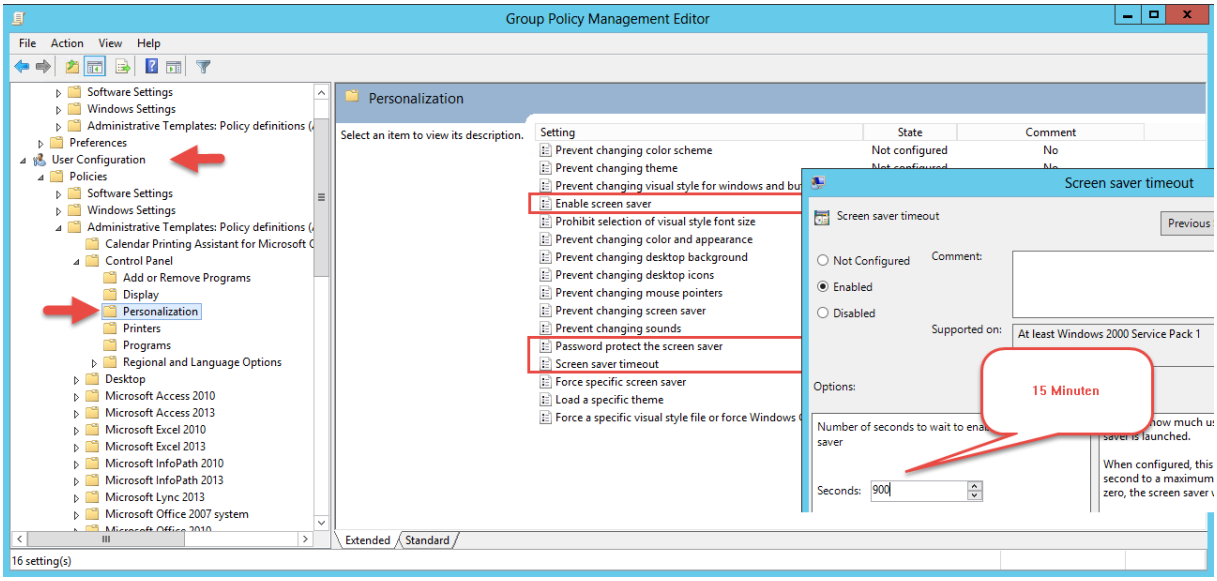


German:

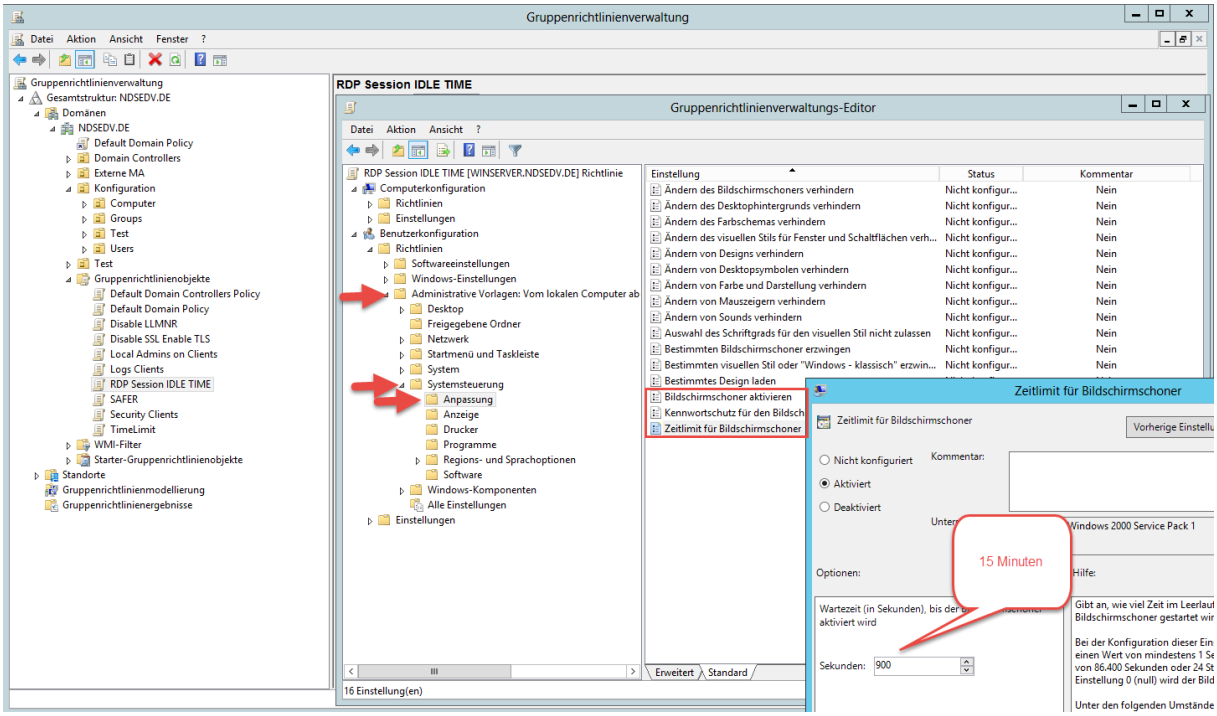


RDP Session IDLE TIME

Der konfigurierte Benutzerteil (Screensaver) der über die Aktivierung der Loopback Verarbeitung berücksichtigt wird.



German:

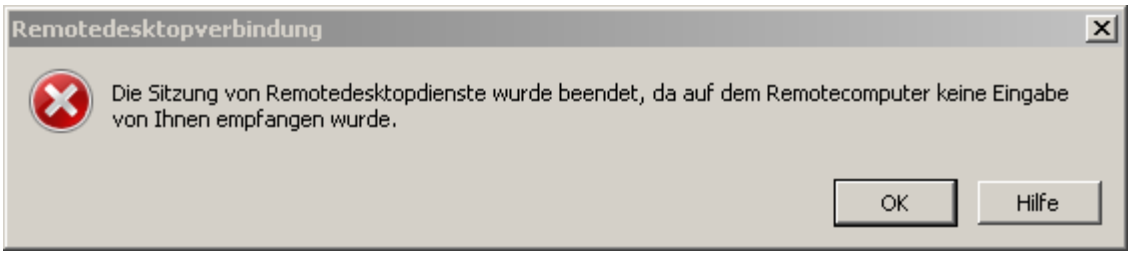


RDP Session IDLE TIME

IDLE TIME:

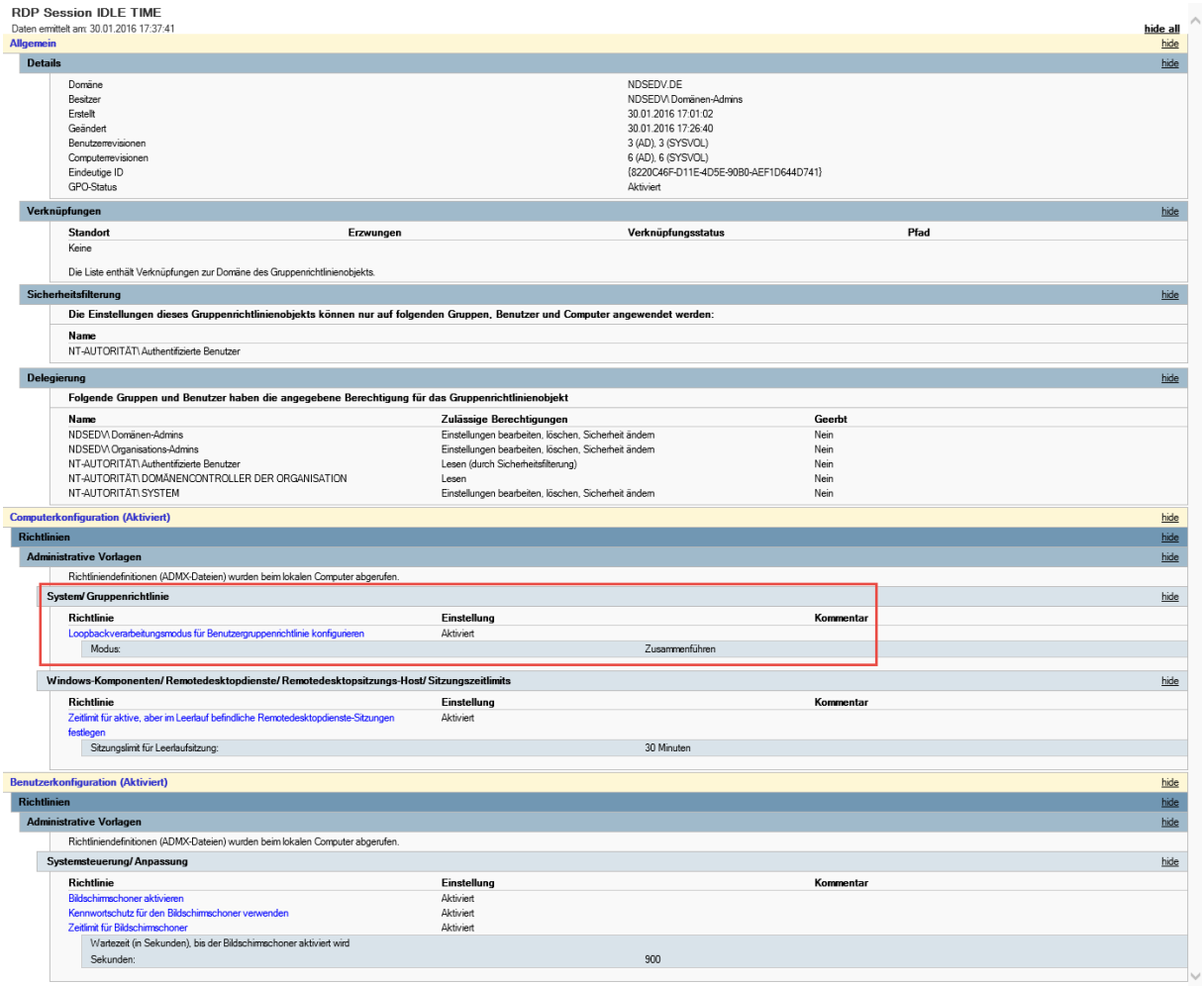
Nach einer IDLE TIME von 15 Minuten wird der Bildschirm gesperrt und durch eine Passwortabfrage geschützt.

Nach einer IDLE TIME von 30 Minuten wird die Session getrennt aber aktive Anwendungen werden nicht unterbrochen.



RDP Session IDLE TIME

GPO Bericht:



RDP Session IDLE TIME

Daten ermittelt am: 30.01.2016 17:37:41

hide all

Allgemein hide

Details hide

Domäne	NDSEDV.DE
Besitzer	NDSEDV\ Domänen-Admins
Erstellt	30.01.2016 17:01:02
Geändert	30.01.2016 17:26:40
Benutzerrevisionen	3 (AD), 3 (SYSVOL)
Computerrevisionen	6 (AD), 6 (SYSVOL)
Eindeutige ID	{8220C46F-D11E-4D5E-90B0-AEF1D644D741}
GPO-Status	Aktiviert

Verknüpfungen hide

Standort	Erzwungen	Verknüpfungsstatus	Pfad
Keine			

Die Liste enthält Verknüpfungen zur Domäne des Gruppenrichtlinienobjekts.

Sicherheitsfilterung hide

Die Einstellungen dieses Gruppenrichtlinienobjekts können nur auf folgenden Gruppen, Benutzer und Computer angewendet werden:

Name
NT-AUTORITÄT\Authentifizierte Benutzer

Delegierung hide

Folgende Gruppen und Benutzer haben die angegebene Berechtigung für das Gruppenrichtlinienobjekt

Name	Zulässige Berechtigungen	Geerbt
NDSEDV\Domänen-Admins	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
NDSEDV\Organisations-Admins	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
NT-AUTORITÄT\Authentifizierte Benutzer	Lesen (durch Sicherheitsfilterung)	Nein
NT-AUTORITÄT\DOMÄNENCONTROLLER DER ORGANISATION	Lesen	Nein
NT-AUTORITÄT\SYSTEM	Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein

Computerkonfiguration (Aktiviert) hide

Richtlinien hide

Administrative Vorlagen hide

Richtliniendefinitionen (ADMX-Dateien) wurden beim lokalen Computer abgerufen.

System/ Gruppenrichtlinie hide

Richtlinie	Einstellung	Kommentar
Loopbackverarbeitungsmodus für Benutzergruppenrichtlinie konfigurieren	Aktiviert	
Modus:	Zusammenführen	

Windows-Komponenten/ Remotedesktopdienste/ Remotedesktopsitzungs-Host/ Sitzungszeitlimits hide

Richtlinie	Einstellung	Kommentar
Zeitlimit für aktive, aber im Leerlauf befindliche Remotedesktopdienste-Sitzungen festlegen	Aktiviert	
Sitzungslimit für Leerlaufsitzung:	30 Minuten	

Benutzerkonfiguration (Aktiviert) hide

Richtlinien hide

Administrative Vorlagen hide

Richtliniendefinitionen (ADMX-Dateien) wurden beim lokalen Computer abgerufen.

Systemsteuerung/ Anpassung hide

Richtlinie	Einstellung	Kommentar
Bildschirmschoner aktivieren	Aktiviert	
Kennwortschutz für den Bildschirmschoner verwenden	Aktiviert	
Zeitlimit für Bildschirmschoner	Aktiviert	
Wartezeit (in Sekunden), bis der Bildschirmschoner aktiviert wird		
Sekunden:	900	

Optionale Informationen:

Aktivieren des Screensavers über die Registry:

```
Reg add "HKEY_CURRENT_USER\Control Panel\Desktop" /v ScreenSaveActive /t REG_SZ /d 1 /f
```

Deaktivieren des Screensavers über die Registry:

```
Reg add "HKEY_CURRENT_USER\Control Panel\Desktop" /v ScreenSaveActive /t REG_SZ /d 1 /f
```

Setzen des Time-outs:

```
Reg add "HKEY_CURRENT_USER\Control Panel\Desktop" /v ScreenSaveTimeOut /t REG_SZ /d 0 /f
```

Aktivieren eines passwortgeschützten Screensaver:

```
Reg add "HKEY_CURRENT_USER\Control Panel\Desktop" /v ScreenSaverIsSecure /t REG_SZ /d 1 /f
```

Deaktivieren eines passwortgeschützten Screensaver:

RDP Session IDLE TIME

Reg add "HKEY_CURRENT_USER\Control Panel\Desktop" /v ScreenSaverIsSecure /t REG_SZ /d 1 /f

In der Registry finden wir die Einstellungen unter folgenden Pfad:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Control Panel\Desktop