

- netstat -t (shows active ports and programs running it)

- netstat -naob

## List of Common TCP/IP port numbers

80 + 443 are  
key web servers

For those of you who configure firewalls, routers, port forwarding, and applications connectivity, this regularly updated document lists all standard, common, well known, de-facto, as well as application specific TCP/IP PC port numbers used around the world.

The port numbers specifically highlighted in yellow in the port list below, indicate International Standards ports, some de-facto standard ports, or simply very well-known ports.

Port	Type	Application
<b>Port 21</b>	International Standard	<b><u>FTP port</u></b> This is the port used for all FTP based file transfers, such as with programs like FTP Voyager, WS_FTP, Cute FTP, FTP NOW, and many more. (FTP = File Transfer Protocol).
<b>Port 22</b>	International Standard	<b><u>SSH Server Listening port</u></b> Port used by Secure Shell servers, SSH, to listen for incoming connections.
<b>Port 23</b>	International Standard	<b><u>Telnet port</u></b> The port used by all Telnet applications.
<b>Port 25</b>	International Standard	<b><u>SMTP mail port</u></b> Standard port used for SMTP mail delivery. This is the outgoing mail port used by email programs such as Outlook Express, Outlook, FoxMail, and hundreds more, and it is also the SMTP Outgoing port used by mail servers such as Axigen Mail Server, CMailServer, Lotus Notes, MailEnable, Merak Mail Server, Microsoft Exchange, Novell GroupWise, Qmail, PostCast Server, PostFix, SendMail, SurgeMail, TFS Secure Message Server, WinMail, or any other SMTP / ESMTP standards compliant e-mail MTA (Message Transfer Agent).
<b>Port 42</b>	Microsoft	<b><u>WINS Replication port</u></b> Port used to replicate NETBIOS name tables from one Windows server to another (see port 137 also)
<b>Port 43</b>	International Standard	<b><u>WHOIS port</u></b> Port used for "Whols" requests (for the retrieval of domain name information) to whois servers.
<b>Port 53</b>	International Standard	<b><u>DNS port for DNS requests &amp; replies</u></b> This port is used by clients and servers when exchanging Domain Name information and routing. (DNS = Domain Name Server).

No? (unless said)

No No

★

incoming + outgoing

Port	Type	Application
<b>Port 67</b>	International Standard	<u>DHCP port for DHCP requests &amp; replies</u> This is the port used by the DHCP server and clients when the clients checks with the DHCP server for a new lease and the allocation of an IP address. (DHCP = <u>D</u> ynamic <u>H</u> ost <u>C</u> onfiguration <u>P</u> rotocol).
<b>Port 79</b>	International Standard	<u>Finger command for SMTP</u> <u>Mailservers – ETRN Finger port</u> Port used by SMTP mail servers to send ETRN Finger commands to message queues servers so that those message queues servers know that the mail servers are online and ready to accept queued up mail. In short : this is the port which your email server will use to send an ETRN command to your web hosting company's mail servers so that they deliver to you any waiting incoming mail.
<b>Port 80</b>	International Standard	<u>HTTP port – Internet traffic</u> The port through which most Internet traffic goes through, through HTTP requests. This is the port which web browsers use to browse the web.
<b>Port 102</b>	International Standard	<u>X.400 port</u> X.400 is one of the earliest standards for communications between Message Handling Systems (MHS) in pre-Internet days. As a result X.400 includes provisions for the network communications to include information about the intended destination medium for the message (e.g : email, fax, telex, etc...). In the Windows world this port is used by default by Microsoft Exchange Server MTAs ( <u>M</u> essage <u>T</u> ransfer <u>A</u> gent) to communicate with each other on internal networks with multiple Exchange servers.
<b>Port 110</b>	International Standard	<u>POP3 port</u> Standard port used for POP3 mail delivery and collection. This is the port normally called the Incoming Mail port in email programs such as Outlook Express, Microsoft Outlook, FoxMail, and others.

Port	Type	Application
<b>Port 115</b>	International Standard	<p><u>SFTP port (Secure File Transfer Protocol)</u></p> <p>Port used for FTP file transfers and modifications over a Secure Shell connection (SSH). This is sometimes mistakenly called "FTP over SSH" which it is not – it is actually a completely new file transfer protocol which includes additional features such as error detection, resumption of interrupted transfers, remote file removal, and enumeration (listing) of remote folders and files. Additionally, as the protocol operates within the SSH protocol which secures the connection through authentication and encryption, this protocol has the additional advantage of operating within a secure environment, something which basic FTP lacks totally (passwords and files are sent as clear text which can easily be intercepted and deciphered by snooping programs).</p>
<b>Port 119</b>	International Standard	<p><u>Newsgroups port</u></p> <p>Port used for newsgroups access.</p>
<b>Port 123</b>	International Standard	<p><u>Network Time Protocol port (NTP)</u></p> <p>Port used for checking and synchronising time with another computer (Time Server). For example, this is the port which Windows XP and Windows Vista use when you configure the clock to automatically synchronize itself with a time server on the Internet. Ditto when you configure a Windows Server to synchronize its time over the Internet.</p>
<b>Port 135</b>	Microsoft	<p><u>RPC Locator Service port</u></p> <p>The RPC locator Service (Remote Procedure Call) maintains a list of networked services that support RPC and DCOM standards. This list holds information regarding which ports and IP addresses the services are currently running on or listening on. Thanks to this list, other computers can query this service to find the details needed to connect to a desired RPC service.</p>
<b>Port 137</b>	Microsoft	<p><u>NetBIOS Name service port / WINS</u></p> <p>Port used by the NetBIOS protocol to find other computers on a workgroup network. On a Peer to Peer network this will be done via broadcast.</p> <p>If a Windows 2000 server or newer is in place, the discovery of other computers can be done with a centralised database called a WINS server (Windows Internet Naming Service) thereby reducing latency and bandwidth usage on the network.</p> <p>This is analogous to DNS for Internet domain names and Microsoft 2000 / 2003 Domains.</p>

Can sync up  
to get exact  
time

Port	Type	Application
<b>Port 143</b>	International Standard	<p><b><u>Internet Message Access Protocol 4 (IMAP4 port)</u></b></p> <p>This port is used by IMAP4 servers.</p> <p>IMAP is a method of accessing emails stored remotely on a mail server (a mailbox). This could be a mailbox at an ISP or a corporate mail server. IMAP4 is "the other" message access protocol – the first one, and most known, being POP3. IMAP works differently from POP3 : the connection to the remote mailbox is constant compared to the Connect-GetMessages-CloseConnection method of POP3. IMAP allows more than one email client to be connected to the same mailbox at the same time – as a direct result it is the protocol of choice for hand-held devices like BlackBerrys as you can have your laptop, desktop PC, and BlackBerry all connected to your mailbox at the same time, something which is not possible with POP3 which requires exclusive access. Another major plus point of IMAP is the ability to retrieve parts of the email, such as the subject only, the message body only, or the attachments only – this is another reason for it being the protocol of choice for devices like BlackBerrys where the user can have the device configured to download and show only the message subjects and when the user decides to open the email in full, then at that point the device requests, specifically, the only the body of the message. Last but not least, the IMAP protocol includes the provision of message status flags which let the remote client know whether a message has been read, deleted, replied to, or forwarded – again, this is crucial to BlackBerry-type devices as that is how the IMAP server can synchronize messages between the device, the server, and any other device simultaneously accessing the same mailbox.</p>
<b>Port 161</b>	International Standard	<p><b><u>Simple Network Management Protocol (SNMP port)</u></b></p> <p>UDP port used to manage, configure, and gather information about network devices (e.g. Firewalls, Routers) in a unified and uniform manner across a varied range of manufacturers. Most server operating systems, whether Windows or not, provide support for this protocol.</p> <p>Note : Home and Small office devices tend to use UPNP for this purpose.</p>
<b>Port 179</b>	International Standard	<p><b><u>Border Gateway Protocol port</u></b></p> <p>The Border Gateway Protocol (BGP) is a routing protocol used to exchange routing information between routers in autonomous networks.</p>

Port	Type	Application
<b>Port 379</b>	Microsoft	<p><u>Site Replication Services (SRS port)</u></p> <p>TCP Port used by Microsoft Site Replication Services.</p> <p>This services enables LDAP enabled servers to replicate between each other information stored on Microsoft Active Directory domain Controllers and Exchange Servers.</p>
<b>Port 389</b>	International Standard	<p><u>Light Weight Directory Access Protocol port (LDAP port)</u></p> <p>TCP Port used to find and manage network resources on an a hierarchical network systems such as Novell Network Directory Trees (NDS), and Microsoft Active Directory Service Domains.</p>
<b>Port 443</b>	International Standard	<p><u>Secure HTTP traffic port (SSL port)</u></p> <p>This is the default port used for SSL encrypted communications (SSL = Secure Socket Layer), such as, for example, when you login to a secure site to purchase something. From a System Administrator's viewpoint, this is the port that is used for incoming and outgoing SSL connections.</p>
<b>Port 445</b>	International Standard	<p><u>Microsoft Active Directory and SMB Protocol port</u></p> <p>This port is used by Microsoft Active Directory services and Microsoft SMB (Server Message Block) protocols. SMB is also known as "Microsoft Windows Network" and is the main protocol used by Microsoft Server Operating Systems for client/server access, and file and printer sharing.</p>
<b>Port 465</b>	Google	<p><u>Google Mail Outgoing Mail Server</u></p> <p>Google uses this non-standard port for its Outgoing Mail Server for Google Mail. Use this port, smtp.gmail.com, and SSL connection (SMTP Server Authentication) when configuring your email client for Google Mail (GMAIL).</p>
<b>Port 636</b>	International Standard	<p><u>LDAP over SSL</u></p> <p>TCP Port used for Lightweight Directory Access Protocol over Secure Socket Layer connections.</p> <p>This a standard added to LDAP to prevent the interception of information and credentials using the LDAP protocol.</p> <p>This standard is used by Microsoft Exchange server and many other LDAP enabled server applications.</p> <p>SEE LDAP PORT: 389</p>

★ encrypted  
version of 80

shouldn't be  
open to web

Port	Type	Application
<b>Port 993</b>	International Standard	<u>Secure Internet Message Access Protocol port (Secure IMAP port)</u> TCP Port used for SSL Secured IMAP 4 access. See IMAP4 Port: 143.
<b>Port 995</b>	Google	<u>Google Mail Incoming POP3 Mail Server (GMAIL port)</u> Google uses this non-standard port for its POP3 Incoming Mail Server for Google Mail (GMAIL). Use this port, pop.gmail.com, and SSL connection when configuring your email client.
<b>Port 1026</b>	Novell  Microsoft	<u>Calendar Access Protocol port (CAP)</u> Port used by Novell GroupWise for its Calendar Access Protocol.  On some <b>Windows 2000</b> servers port 1026 is used by the Windows Task Scheduler or other Windows services.
<b>Port 1080</b>	De-Facto Standard	<u>SOCKS / Online Chatting / Hotmail</u> This port is used mainly by applications such as ICQ, AOL Instant Messenger for online chatting. It is also used by Hotmail.
<b>Port 1090</b>	De-Facto Standard	<u>Real Audio port</u> Port used by Real Audio video and audio streaming applications.
<b>Port 1433</b>	Microsoft	<u>SQL Server Port &amp; SQL Server Replication Port</u> Used by Microsoft SQL Server 6 and above for SQL replication between SQL servers.
<b>Port 1434</b>	Microsoft	<u>SQL Server Monitoring Port</u> Used by Microsoft SQL Server to monitor SQL server performance.
<b>Port 1521</b>	Oracle	<u>Default Oracle port</u> Default port for connection to an Oracle database server.
<b>Port 1677</b>	Novell	<u>Novell GroupWise</u> Standard port used by Novell GroupWise for TCP/IP communications between clients and agents and the GroupWise Post Office Agent (POA).

investigate  
unless says  
OK

check base

check  
(database)

Port	Type	Application
<b>Port 1701</b>	International Standard	<p><b><u>Layer Two Tunneling Protocol port (L2TP port)</u></b></p> <p>A tunnelling and encryption standard used to connect two Private Business networks together over an Internet connection to create a Virtual Private Network (VPN).</p> <p>This protocol is seen as the replacement to PPTP (port <b>1723</b> listed below).</p>
<b>Port 1720</b>	De-Facto Standard	<p><b><u>H.323 port</u></b></p> <p>Port used for video conferencing equipment which uses the H.323 protocol.</p>
<b>Port 1723</b>	International Standard	<p><b><u>Point to Point Tunneling Protocol port (PPTP port)</u></b></p> <p>A tunnelling and encryption standard used to connect two Private Business networks together over an Internet connection (creating one Virtual Private Network). This is the default protocol for establishing a VPN on Windows 2000 Server.</p>
<b>Port 1900</b>	Microsoft	<p><b><u>Media Center Extender – Xbox 360 port</u></b></p> <p>UDP inbound. Port used by Microsoft's Xbox 360 when linking to Media Center.</p>
<b>Port 2409</b>	SPAMFighter	<p><b><u>SPAMFighter Content Classification port</u></b></p> <p>UDP inbound and Outbound. Port used by the SPAMFighter software to communicate with its servers in order to determine which emails are spam or not.</p>
<b>Port 3101</b>	Research in Motion	<p><b><u>Blackberry Enterprise Server (BES) Synchronization Port (BES port)</u></b></p> <p>If you have an outbound firewall, then you will need to open this port (TCP) to enable the Blackberry Enterprise Server to synchronize with the Blackberry devices. Additionally, depending on the configuration of your particular site, you may also need to port forward port 3101 from your router to the Blackberry Enterprise Server.</p>
<b>Port 3306</b>	MySQL AB	<p><b><u>Default MySQL Port</u></b></p> <p>Default port for connection to a MySQL database server.</p>

Not bad  
unless  
you're  
off it

Port	Type	Application
<b>Port 3389</b> ★	Microsoft	<u>Remote Desktop Port &amp; Terminal Services Port</u>  <b>TCP Inbound &amp; Outbound.</b> Default port used by Windows XP Remote Desktop Connection and Microsoft Terminal Server for Remote Desktop Connections and/or Terminal Services sessions. For added security it is recommended to change the Remote Desktop port from its default to a value of your choice – this can be changed in the Registry at <b>HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber</b> (the "RDP-Tcp" part may have a different name if you renamed your Terminal Server \ Remote Desktop connection).
<b>Port 3390</b>	Microsoft	<u>Media Center Extender – Xbox 360 port</u>  <b>TCP Inbound.</b> Port used by Microsoft's Xbox 360 when linking to Media Center.
<b>Port 3535</b>	GoDaddy	<u>GoDaddy Secure SMTP Relay port</u>  Port used by GoDaddy customers for email sending using SMTP relay with authentication over any ISP connection via GoDaddy's Outgoing Mail Server, <b>smtpout.secureserver.net</b> . This enables GoDaddy customers to email from anywhere without having to constantly change their email settings to reflect the SMTP server corresponding to the Internet connection they are using at the time – instead they can email through GoDaddy's SMTP Relay regardless of where they are.
<b>Port 4321</b>	De Facto Standard	<u>RWHOIS port</u>  Port used for "RWhois" requests.
<b>Port 4664</b>	Google	<u>Google Desktop Search port</u>
<b>Port 5190</b>	America On Line	<u>AOL Instant Messenger port</u>  Port used by AIM, the AOL Instant Messenger software.
<b>Port 5500</b>	DualDesk	<u>DualDesk port</u>  Default port used by the DualDesk remote control software.
<b>Port 5631</b>	PCAnywhere	<u>PCAnywhere 5631 TCP incoming port</u>  Port on which a Symantec PC Anywhere host accepts incoming PC Anywhere connections and then continues to communicate with the remote PC. If you have a PC Anywhere host behind a firewall or firewalled router, then you need to allow (and possibly port forward) incoming TCP connections on this port.



Port	Type	Application
Port 3389 ★	Microsoft	<u>Remote Desktop Port &amp; Terminal Services Port</u>  <b>TCP Inbound &amp; Outbound.</b> Default port used by Windows XP Remote Desktop Connection and Microsoft Terminal Server for Remote Desktop Connections and/or Terminal Services sessions. For added security it is recommended to change the Remote Desktop port from its default to a value of your choice – this can be changed in the Registry at <b>HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber</b> (the "RDP-Tcp" part may have a different name if you renamed your Terminal Server \ Remote Desktop connection).
Port 3390	Microsoft	<u>Media Center Extender – Xbox 360 port</u>  <b>TCP Inbound.</b> Port used by Microsoft's Xbox 360 when linking to Media Center.
Port 3535	GoDaddy	<u>GoDaddy Secure SMTP Relay port</u>  Port used by GoDaddy customers for email sending using SMTP relay with authentication over any ISP connection via GoDaddy's Outgoing Mail Server, <b>smtpout.secureserver.net</b> . This enables GoDaddy customers to email from anywhere without having to constantly change their email settings to reflect the SMTP server corresponding to the Internet connection they are using at the time – instead they can email through GoDaddy's SMTP Relay regardless of where they are.
Port 4321	De Facto Standard	<u>RWHOIS port</u>  Port used for "RWhois" requests.
Port 4664	Google	<u>Google Desktop Search port</u>
Port 5190	America On Line	<u>AOL Instant Messenger port</u>  Port used by AIM, the AOL Instant Messenger software.
Port 5500	DualDesk	<u>DualDesk port</u>  Default port used by the DualDesk remote control software.
Port 5631	PCAnywhere	<u>PCAnywhere 5631 TCP incoming port</u>  Port on which a Symantec PC Anywhere host accepts incoming PC Anywhere connections and then continues to communicate with the remote PC. If you have a PC Anywhere host behind a firewall or firewalled router, then you need to allow (and possibly port forward) incoming TCP connections on this port.


Not bad  
 unless  
 guys are  
 off it

Port	Type	Application
<b>Port 5632</b>	PCAnywhere	<u>PCAnywhere 5632 UDP incoming port</u> Port used by Symantec's PC Anywhere for the streaming of screen updates during a PC Anywhere session. If you have a PC Anywhere host behind a firewall or firewalled router, then you need to allow (and possibly port forward) incoming UDP connections on this port.
<b>Port 5900</b>	RealVNC Ltd (De-facto VNC default port)	<u>RealVNC Default Remote Control Port</u> This is the default RealVNC port for port forwarding to the RealVNC host. You should always change this port from its default as it is a well-known port for all VNC remote control programs and it will therefore be one of the first targets of hackers !
<b>Port 7070</b>	Real Networks	<u>Real Streaming Audio port</u> Port used by Real Networks' audio streaming servers.
<b>Port 7100</b>	Novell	<u>Novell GroupWise</u> Standard port used by Novell GroupWise for TCP/IP communications between the Message Transfer Agent (MTA) and other agents.
<b>Port 8000</b>	Mirra Inc	<u>Mirra Personal Server Communications port</u> Port used by both the Mirra Client running on the PC, and the Mirra Personal Server, to communicate with each other. This is a TCP port.
<b>Port 8080</b>	International Standard	<u>HTTP Internet traffic port</u> The other port through which HTTP Internet traffic also goes through.
<b>Port 8799</b>	Vodafone UK	<u>GPRS Internet Access Proxy port</u> Port used for GPRS Internet Browsing on the Vodafone UK mobile phone network. If you are on Vodafone you typically need to configure your phone to access the Internet via a proxy on port 8799. The proxy address is : 212.183.137.12:8799.
<b>Port 8880</b>	De Facto Standard	<u>CDDDB port</u> Port used by CD mastering software to communicate with an Internet based CDDDB server for requests about artist and track names.
<b>Port 9100</b>	Google	<u>Google Web Accelerator port</u> Port used by Google Web Acceleration technology. Google Web Accelerator supports <u>natively</u> only Internet Explorer and FireFox at the time of writing, 2-Sep-2006. Other browsers need to have their HTTP Proxy configured to 127.0.0.1:9100.

  
 No. No. Port 5900

Port	Type	Application
<b>Port 5632</b>	PCAnywhere	<u>PCAnywhere 5632 UDP incoming port</u> Port used by Symantec's PC Anywhere for the streaming of screen updates during a PC Anywhere session. If you have a PC Anywhere host behind a firewall or firewalled router, then you need to allow (and possibly port forward) incoming UDP connections on this port.
<b>Port 5900</b>	RealVNC Ltd (De-facto VNC default port)	<u>RealVNC Default Remote Control Port</u> This is the default RealVNC port for port forwarding to the RealVNC host. You should always change this port from its default as it is a well-known port for all VNC remote control programs and it will therefore be one of the first targets of hackers !
<b>Port 7070</b>	Real Networks	<u>Real Streaming Audio port</u> Port used by Real Networks' audio streaming servers.
<b>Port 7100</b>	Novell	<u>Novell GroupWise</u> Standard port used by Novell GroupWise for TCP/IP communications between the Message Transfer Agent (MTA) and other agents.
<b>Port 8000</b>	Mirra Inc	<u>Mirra Personal Server Communications port</u> Port used by both the Mirra Client running on the PC, and the Mirra Personal Server, to communicate with each other. This is a TCP port.
<b>Port 8080</b>	International Standard	<u>HTTP Internet traffic port</u> The other port through which HTTP Internet traffic also goes through.
<b>Port 8799</b>	Vodafone UK	<u>GPRS Internet Access Proxy port</u> Port used for GPRS Internet Browsing on the Vodafone UK mobile phone network. If you are on Vodafone you typically need to configure your phone to access the Internet via a proxy on port 8799. The proxy address is : 212.183.137.12:8799.
<b>Port 8880</b>	De Facto Standard	<u>CDDDB port</u> Port used by CD mastering software to communicate with an Internet based CDDDB server for requests about artist and track names.
<b>Port 9100</b>	Google	<u>Google Web Accelerator port</u> Port used by Google Web Acceleration technology. Google Web Accelerator supports <u>natively</u> only Internet Explorer and FireFox at the time of writing, 2-Sep-2006. Other browsers need to have their HTTP Proxy configured to 127.0.0.1:9100.

  
 No. No. Port 5900



Port	Type	Application
<b>Port 19430</b>	Mirra Inc	<u>Mirra Personal Server Discovery port</u>  This is a <b>UDP</b> port used by the Mirra Client software running on the PC to discover its assigned Mirra Personal Server (Broadcast over UDP).
<b>Port 39720</b>	Lime Wire LLC	<u>LimeWire communications port</u>  This is the default port which the LimeWire peer-to-peer file-sharing program uses (can be changed by the end-user).

ooooooooOooooooooo

# 8 tips to secure IIS installations

You have just finished installing IIS on your Windows OS. You're probably thinking that you can delve into the web development world and forget all about the underlying web server. After all, IIS is a Microsoft product so it should install with the right default configuration settings, right? That is far from true with IIS.

In this article, I will provide 8 tips that you can use to secure IIS installations.


## **Move the `Inetpub` folder to a different drive** *\*Do not do for Cy Per Patricia\**

The `Inetpub` folder is the default location for your web content, IIS logs and so on. By default IIS 7 and upwards install the `Inetpub` folder in the system drive. It's good practice to move the `Inetpub` folder to a different partition so that the web content is separate from the operating system. This folder can be moved after IIS installation is completed. Thomas Deml, IIS Lead Program Manager provided this [batch file](#) to help with the move.

## **Install the appropriate IIS modules**

IIS includes more than 30 [modules](#) – you should only install the ones which are needed by your web applications. Disable any modules that are not required, to minimise the capacity of potential attacks. Periodically review the modules that are installed and enabled and remove any that are no longer required. You can use IIS Manager to list all the modules that are enabled.

1. Open IIS Manager
2. Select the name of the machine to view the modules for the whole machine, or change to the specific web site to view the modules enabled for the selected site
3. Double click on 'Modules'
4. To disable a module, click on the module from the list and select 'Remove' from the Actions pane
5. Confirm the removal by pressing Yes

 **Modules**

Use this feature to configure the native and managed code modules that process requests made to the Web server.

Group by: No Grouping

Name	Code	Module Type	Entry Type
AnonymousAuthenticationModule	%windir%\System32\inetrv\authanon.dll	Native	Local
CustomErrorModule	%windir%\System32\inetrv\custerr.dll	Native	Local
DefaultDocumentModule	%windir%\System32\inetrv\defdoc.dll	Native	Local
DirectoryListingModule	%windir%\System32\inetrv\dirut.dll	Native	Local
HttpCacheModule	%windir%\System32\inetrv\cachhttp.dll	Native	Local
HttpLoggingModule	%windir%\System32\inetrv\loghttp.dll	Native	Local
ProtocolSupportModule	%windir%\System32\inetrv\protsup.dll	Native	Local
RequestFilteringModule	%windir%\System32\inetrv\modiqlt.dll	Native	Local
ServiceModel	System.ServiceModel.Activation.HttpModule, System.ServiceModel, Version=3.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089	Managed	Local
ServiceModel-4.0	System.ServiceModel.Activation.ServiceHttpModule, System.ServiceModel.Activation, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089	Managed	Local
StaticCompressionModule	%windir%\System32\inetrv\compstat.dll	Native	Local
StaticFileModule	%windir%\System32\inetrv\static.dll	Native	Local

Figure 1 – Viewing all the enabled modules from the IIS Manager

## Disable the OPTIONS method

The OPTIONS method provides a list of methods that are supported by the web server. Although this might seem beneficial, it also provides useful information to an attacker. This will provide information to an attacker at the reconnaissance stage of this attack. Therefore it's recommended to disable the OPTIONS method completely. This can be done by denying the OPTIONS verb from the HTTP Verb request filtering rules in IIS.

1. Open IIS Manager
2. Select the name of the machine to configure this globally (or change to the specific web site for which you need to configure this)
3. Double click on 'Request Filtering'
4. Change to the HTTP Verbs tab
5. From the Actions pane, select 'Deny Verb'
6. Insert 'OPTIONS' in the Verb, and press OK to save changes



Figure 2 – Denying the OPTIONS method from the IIS Manager

## Enable Dynamic IP Restrictions

The Dynamic IP Restrictions module helps blocks access to IP addresses that exceed a specified number of requests and thus helps prevent Denial of Service (DoS) attacks. This module will inspect the IP address of each request sent to the web server and will filter these requests in order to temporarily deny IP addresses that follow a particular attack pattern. The Dynamic IP Restrictions module can be configured to block IP addresses after a number of concurrent requests or by blocking IP addresses that perform a number of requests over a period of time. Depending on your IIS version you will need to enable either the 'IP Security' feature or the "IP and Domain Restrictions" as explained in this Microsoft article.

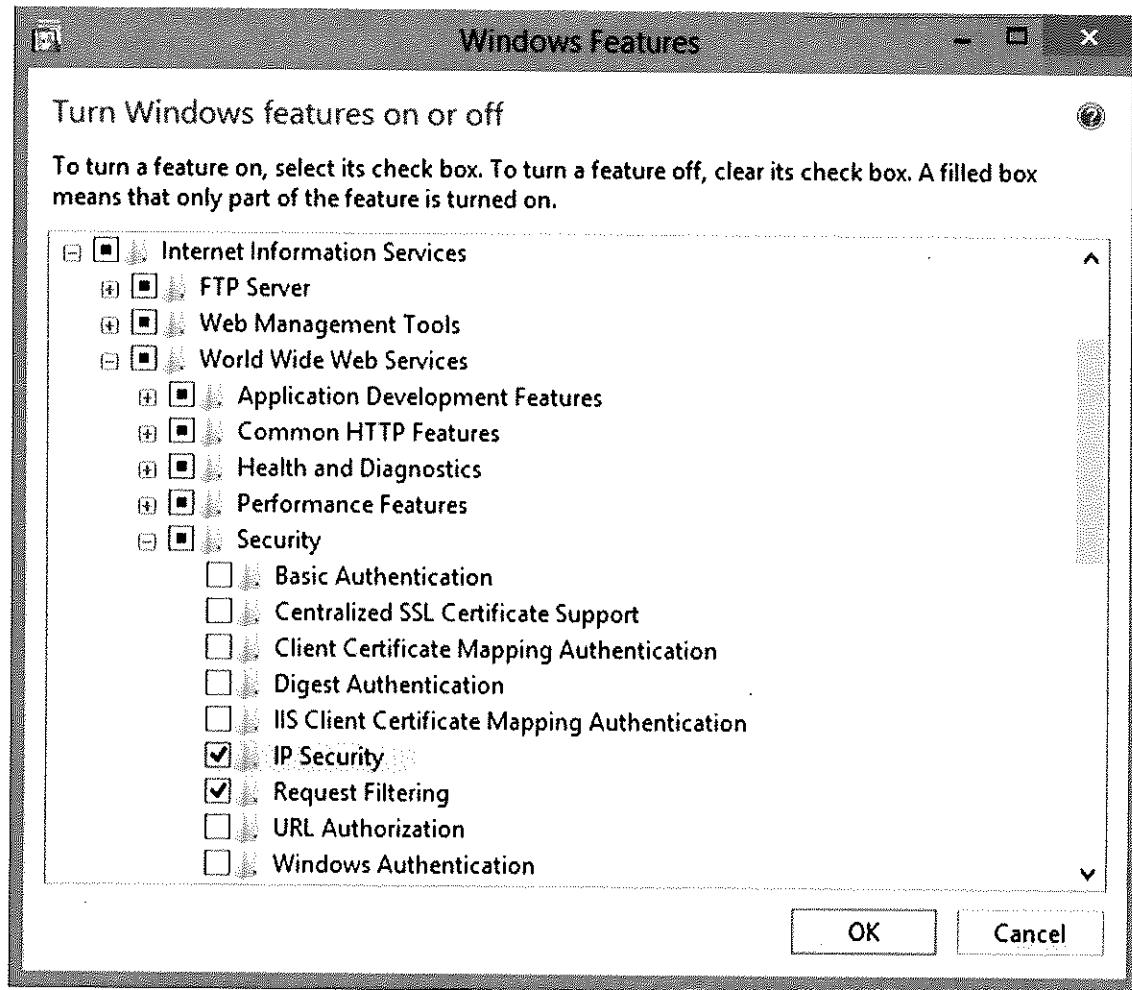


Figure 3 – Enabling the ‘IP Security’ feature to allow for Dynamic IP Restrictions in IIS

This will include the ‘IP Address and Domain Restrictions’ module in the IIS Manager, from where dynamic IP restrictions can be set.

1. Open IIS Manager
2. Select the name of the machine to configure this globally (or change to the specific web site for which you need to configure this)
3. Double click on ‘IP Address and Domain Restrictions’
4. From the Actions pane, select ‘Edit Dynamic Restriction Settings’
5. Modify and set the dynamic IP restriction settings as needed and press OK to save changes



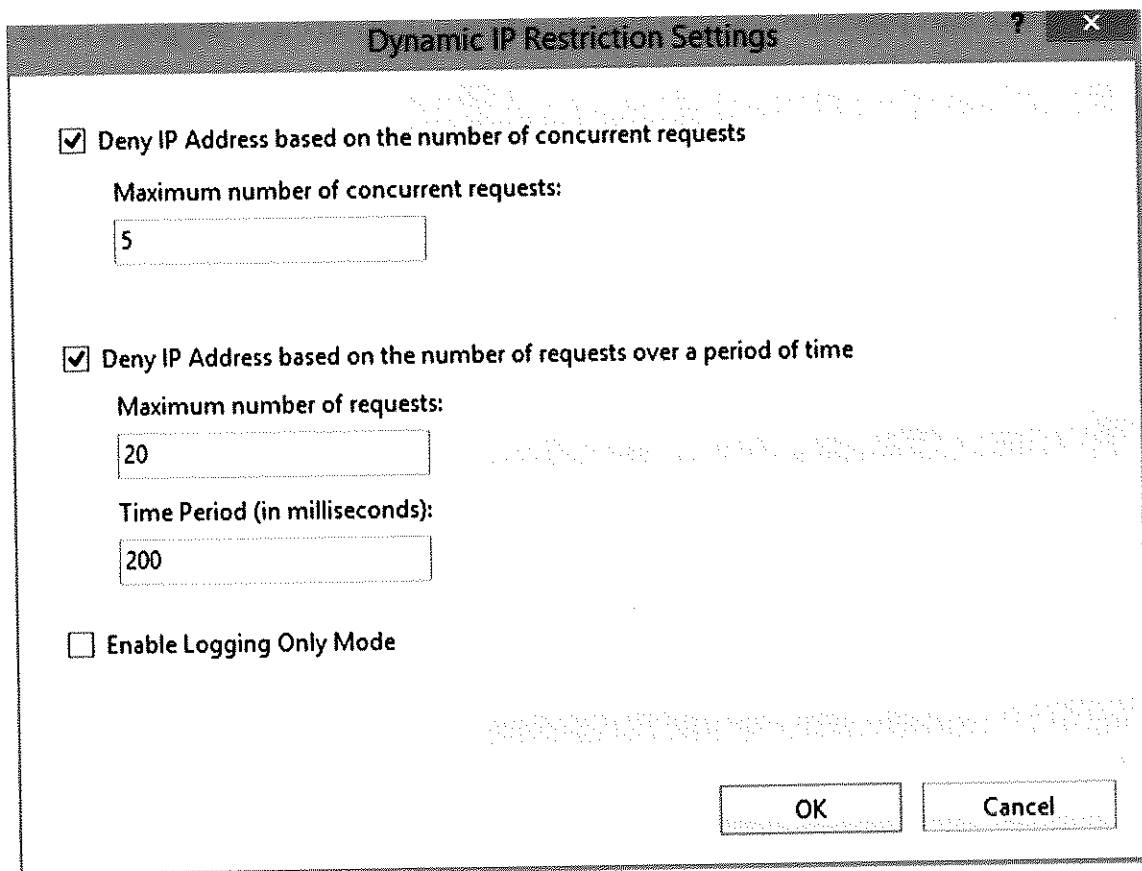


Figure 4 – Dynamic IP Restrictions settings can be modified from the IIS Manager

## Enable and Configure Request Filtering Rules

It is also a good idea to restrict the types of HTTP requests that are processed by IIS. Setting up exclusions and rules can prevent potentially harmful requests from passing through to the server, since IIS can block these requests on the basis of the request filtering rules defined. For example, a rule can be set to filter traffic for SQL Injection attempts. Whilst SQL Injection vulnerabilities should be fixed at source, filtering for SQL Injection attacks is a useful mitigation. This can be set from the Rules tab found in the Request Filtering page in IIS Manager.

1. Open IIS Manager
2. Select the name of the machine to configure this globally (or change to the specific web site for which you need to configure this)
3. Double click on 'Request Filtering'
4. Change to the Rules tab
5. From the Actions pane, select 'Add Filtering Rule'
6. Set the required rules, and press OK to save changes

The rule set in the below screenshot would instruct IIS to check for the provided strings in requests for .asp and .aspx pages. IIS will then block the request if any of these strings are found.

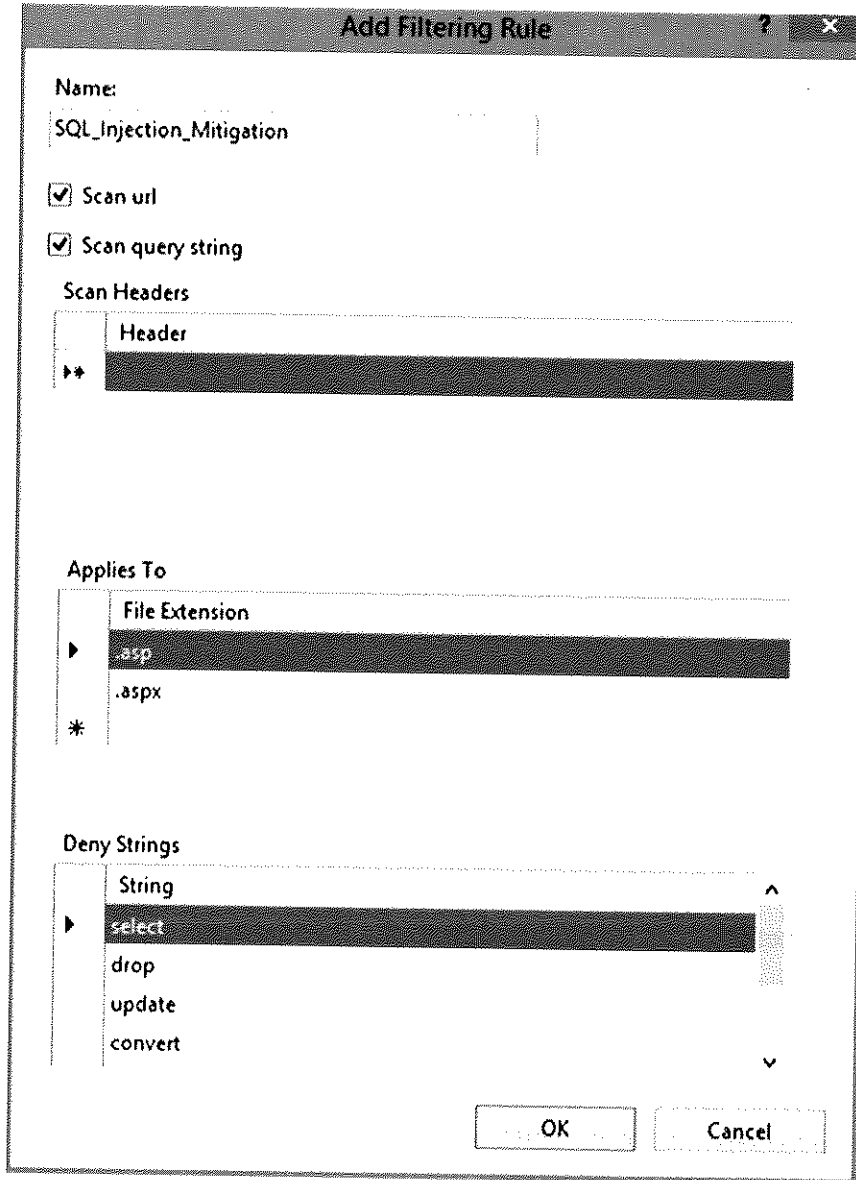


Fig 5 – Request filtering rule that checks for SQL Injection attacks

You can also filter requests that contain things like high-bit characters or double escape characters. This and other similar filtering options are explained at <http://technet.microsoft.com/en-us/library/hh831621.aspx>

## Enable logging *Good One*

Configuring IIS logging will cause IIS to log various information from HTTP requests received by the server. This will come in handy and can give a better understanding of issues that might

have occurred on your website when things go wrong. It's the place where you will start the troubleshooting process in such situations.

The server's logs can also be continuously or periodically monitored in order to review the server's performance and provide optimizations if needed. This can be automated using various server monitoring tools. Make sure to keep a backup of the logs. Microsoft also provide Log Parser, which is a tool that can be used to query and retrieve specific data from IIS logs. Additionally, log consolidation tools prove useful for consolidating and archiving data from logs in a more meaningful way.

IIS logging can be enabled and configured from IIS Manager > select the machine name or the specific site you want to configure > Logging. Since these log files might grow quite large, it would be a good idea to start a new file periodically.

The screenshot shows the 'Logging' configuration page in IIS Manager. The page has a title bar 'Logging' and a subtitle 'Use this feature to configure how IIS logs requests on the Web server.' Below the subtitle, there are several sections: 'One log file per:' with a dropdown menu set to 'Site'; 'Log File' section with 'Format' set to 'W3C' and a 'Select Fields...' button, 'Directory' set to '%SystemDrive%\inetpub\logs\Logfiles' with a 'Browse...' button, and 'Encoding' set to 'UTF-8'; 'Log Event Destination' section with three radio buttons: 'Log file only' (selected), 'ETW event only', and 'Both log file and ETW event'; 'Log File Rollover' section with three radio buttons: 'Schedule:' (selected) with a dropdown menu set to 'Daily', 'Maximum file size (in bytes):', and 'Do not create new log files', and a checkbox 'Use local time for file naming and rollover' which is unchecked. At the bottom, there are two tabs: 'Features View' and 'Content View'. On the right side, there is an 'Actions' pane with buttons: 'Apply', 'Cancel', 'Disable', 'View Log Files...', and 'Help'.

Figure 6 – Logging options in IIS

# Use the Security Configuration Wizard (SCW) and the Security Compliance Manager (SCM)

Both of these Microsoft tools can be used to test your IIS security. The Security Configuration Wizard (SCW) runs different checks and provides advice and recommendations on how to boost your server's security. The Security Compliance Manager (SCM) tool performs security tests on your server and compares server configurations to predefined templates as per industry best practices and security guide recommendations.

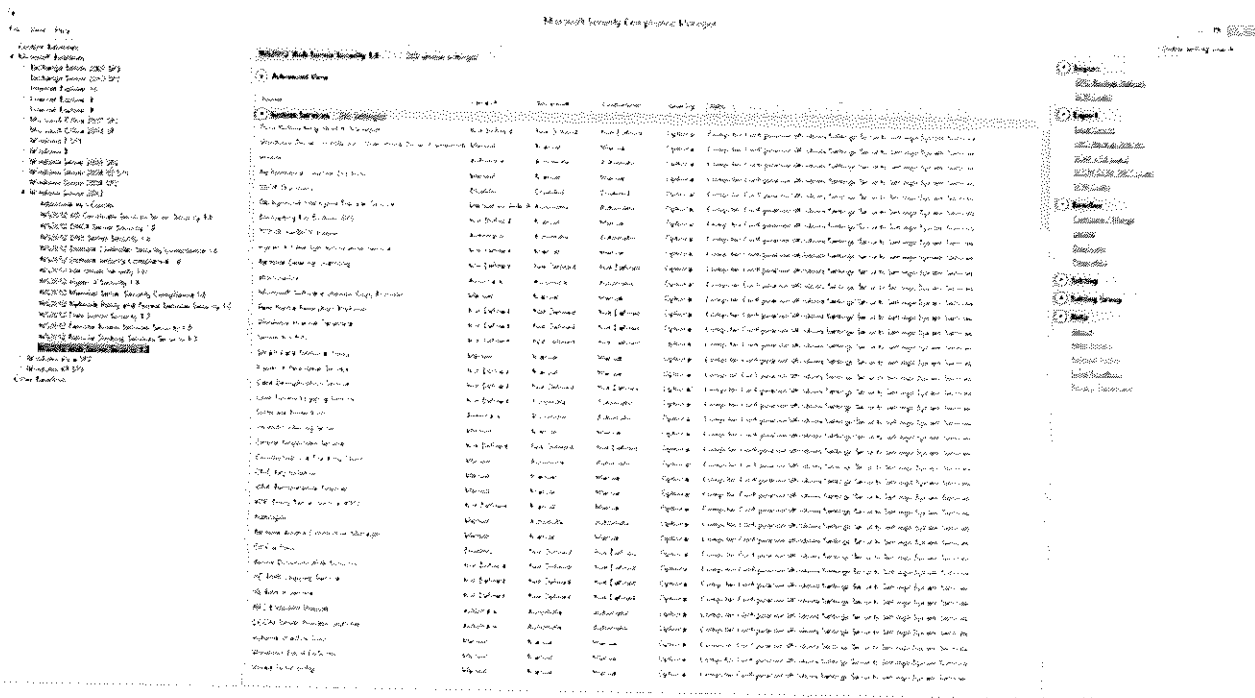


Figure 7 – The Microsoft Security Compliance Manager (SCM) tool

## Updates

Finally, ensure that you keep up to date with the latest updates and security patches. It is interesting how often this basic security requirement is missed. The majority of hacks affecting the web server occur on unpatched servers. This just demonstrates how important it is to always keep your IIS web server up to date.

<https://www.acunetix.com/blog/articles/8-tips-secure-iis-installation/>

(See also: <http://searchsecurity.techtarget.com/feature/Windows-IIS-server-hardening-checklist>)

# Mitigation

The good news is that mitigating these risks can be done by changing 3 settings. The changes are compatible with every supported Microsoft operating system and many 3rd party RDP clients. The settings can be changed via GUI, PowerShell, and Group Policy.

## Set the Security Layer to SSL (TLS 1.0)

This setting requires the use of TLS 1.0 or higher encryption to protect the session as opposed to the legacy RDP encryption. In addition to increasing the strength of the encryption, it also enables the detection of MitM attacks by requiring the server to present a TLS (x.509) certificate as proof of identity. Ideally every server would have a certificate issued from a trusted authority but even when using self-signed certificates this can allow observant users to detect MitM after the first connection. If both the client and the server support and require the use of TLS cipher suites that provide Forward Secrecy (ECDHE, DHE) then sniffed RDP sessions cannot be decrypted after the fact even if the RDP Server's TLS certificate is compromised. Further, any efforts spent hardening the TLS configuration of the server or client will result in better security for their RDP sessions.

In the right environment, this setting will completely mitigate MitM and sniffing risks. It also provides the benefit of being able to assure stake holders and interested 3rd parties such as customers and auditors that their traffic is being protected using well known and widely accepted encryption.

## Enable Network Level Authentication (NLA)

Network Level Authentication requires a user connecting via RDP to authenticate **before** a session is allowed to be established to a server. It can leverage Kerberos, NTLM, and PKI for authentication when those technologies are available. Additionally, due to its use of the Microsoft CredSSP protocol, all of the traffic during the session is sent over TLS 1.0 or higher. This effectively enforces the Security Layer setting discussed above and all that it entails.

The use of NLA completely mitigates the Information Disclosure issue as described above, and **currently** breaks all of the popular RDP brute force tools.

NLA is enabled by default in Windows 2012 R2.

## Set the Encryption Level to High

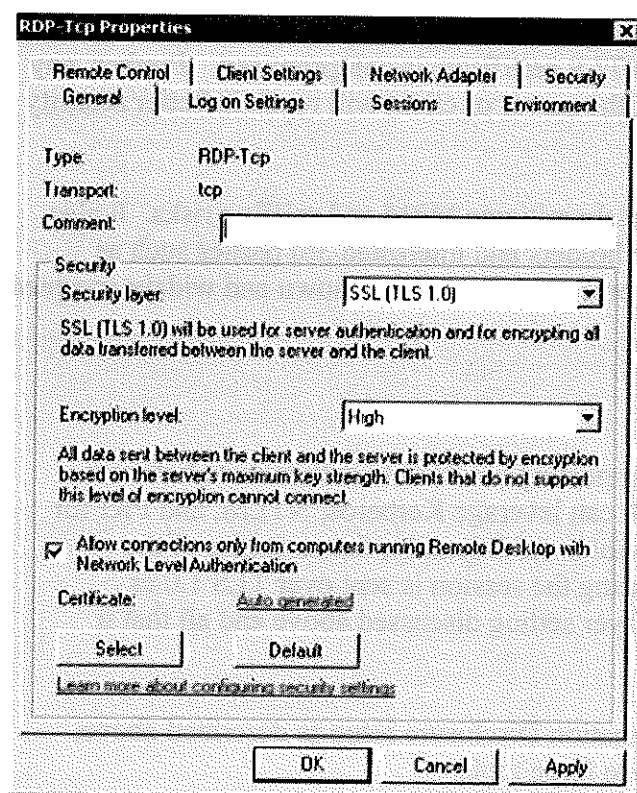
By default, Windows allows the server and client to negotiate the encryption level. Setting Encryption Level to 'High' requires that at least 128 bit encryption is used or the server will not allow the client to connect. Depending on the requirements of the environment, Encryption Level can be set to FIPS instead. This setting doesn't directly address one of the risks above but may make it more resilient to unforeseen downgrade attacks against the deployed cryptography.

# Deployment

The settings can be deployed to the environment in a couple of ways.

## GUI

On Windows 2008 and 2008 R2 the values can be change via the GUI by going to **Start, Administrative Tools, Remote Desktop Services**, and then clicking **Remote Desktop Session Host Configuration**. Under **Connections**, right click on **RDP-tcp** and click **Properties**. All of the settings covered above can be configured on the **General** tab of the resulting window. Once the desired settings are in place, click **Apply**. This change takes effect immediately but does not affect any sessions currently connected. This will allow the new settings to be reverted easily if testing shows that they cause problems.



On Windows 2012 Microsoft has changed the GUI so as to not provide this level of control. As NLA is enabled by default on 2012 this is less of an issue than it would be on 2008 R2.

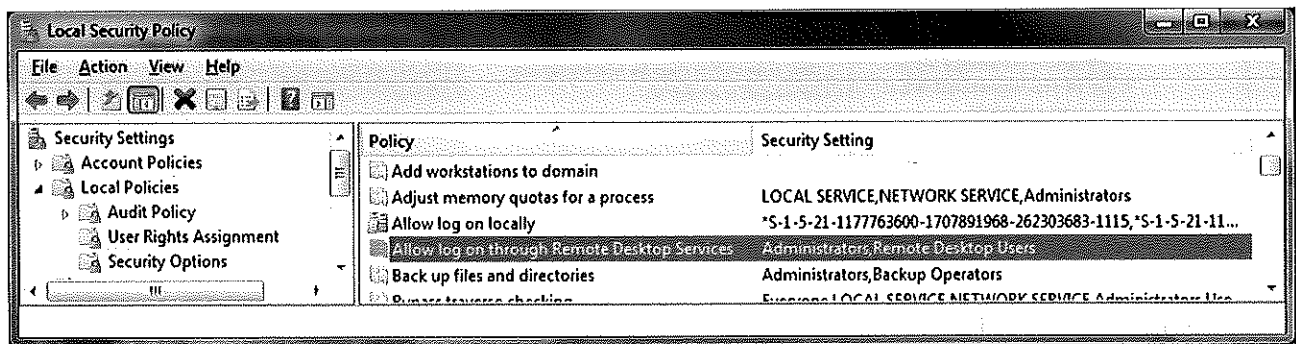
## Limit users who can log in using Remote Desktop

By default, all Administrators can log in to Remote Desktop. If you have multiple Administrator accounts on your computer, you should limit remote access only to those accounts that need it. If Remote Desktop is not used for system administration, remove all administrative access via RDP

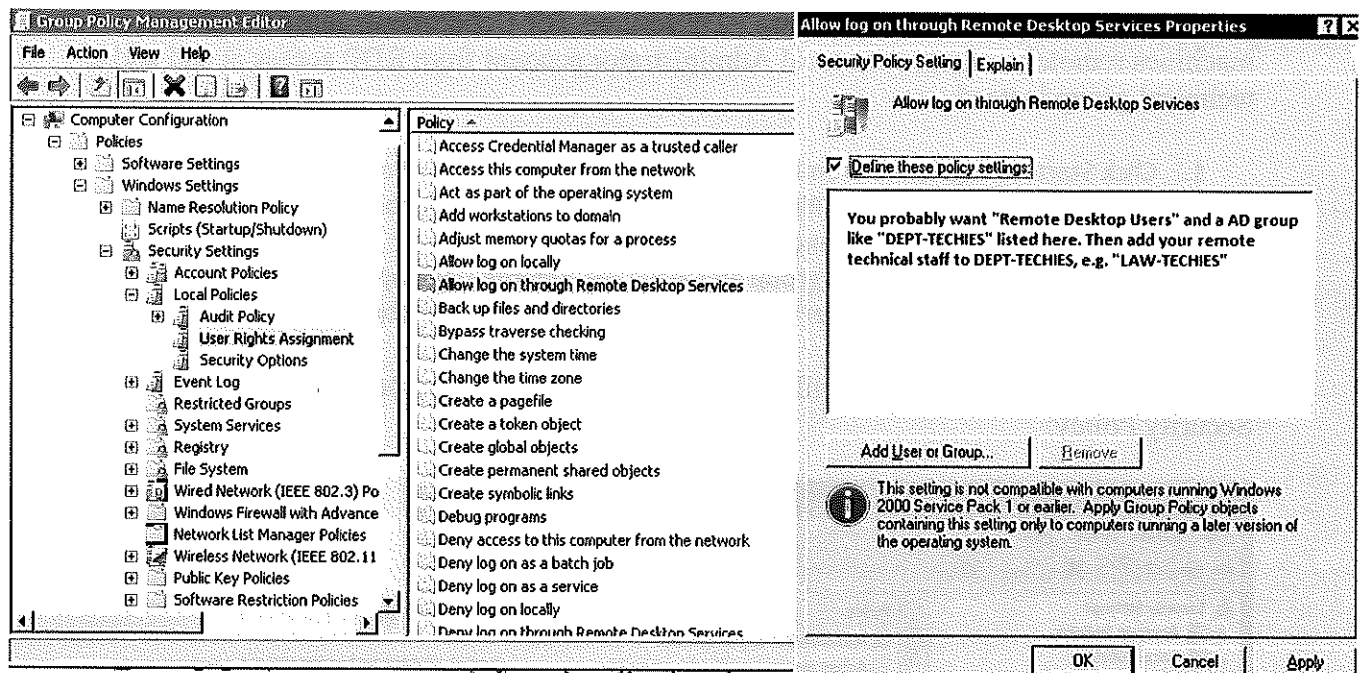
and only allow user accounts requiring RDP service. For Departments that manage many machines remotely, remove the local Administrator account from RDP access at and add a technical group instead.

1. Click Start-->Programs-->Administrative Tools-->Local Security Policy
2. Under Local Policies-->User Rights Assignment, go to "Allow logon through Terminal Services." Or "Allow logon through Remote Desktop Services"
3. Remove the Administrators group and leave the Remote Desktop Users group.
4. Use the System control panel to add users to the Remote Desktop Users group.

A typical MS operating system will have the following setting by default as seen in the Local Security Policy:

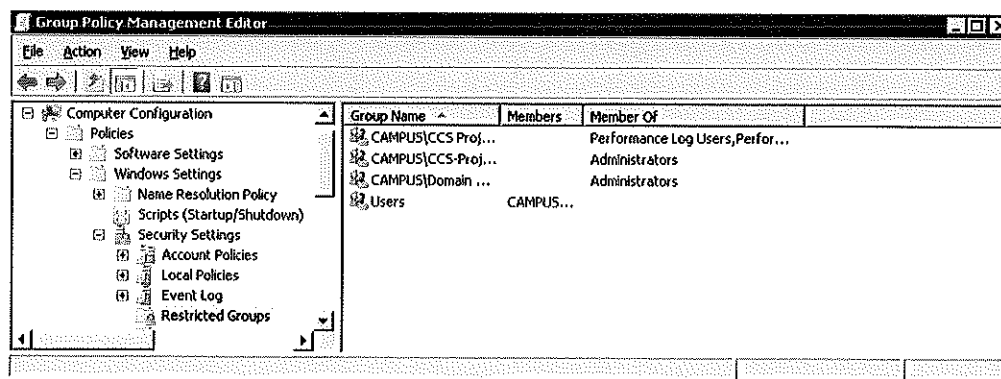


The problem is that "Administrators" is here by default, and your "Local Admin" account is in administrators. Although a password convention to avoid identical local admin passwords on the local machine and tightly controlling access to these passwords or conventions is recommended, using a local admin account to work on a machine remotely does not properly log and identify the user using the system. It is best to override the local security policy with a Group Policy Setting.



To control access to the systems even more, using “Restricted Groups” via Group Policy is also helpful.

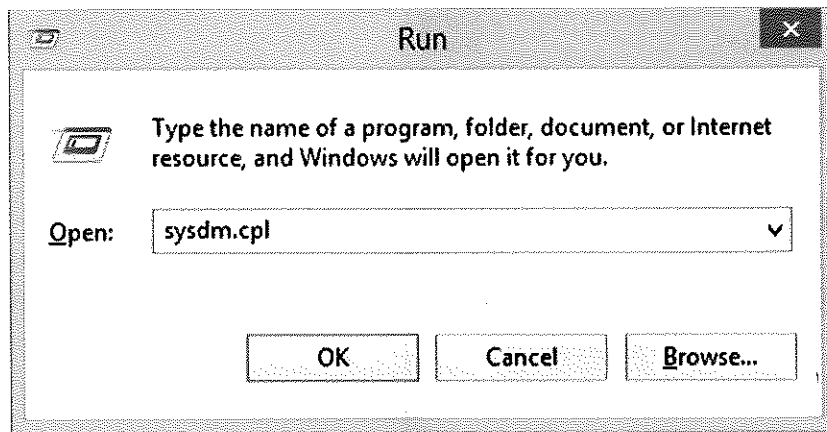
If you use a “Restricted Group” setting to place your group e.g. “CAMPUSLAW-TECHIES” into “Administrators” and “Remote Desktop Users”, your techies will still have administrative access remotely, but using the steps above, you have removed the problematic “local administrator account” having RDP access. Going forward, whenever new machines are added in the OU under the GPO, your settings will be correct.



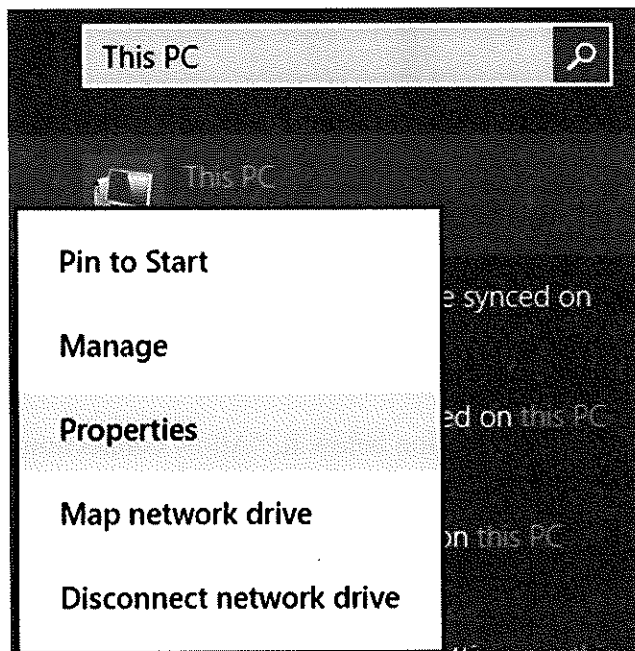
## Enabling Remote Desktop

First, we need to enable Remote Desktop and select which users have remote access to the computer. Hit Windows key + R to bring up a Run prompt, and type “sysdm.cpl.”

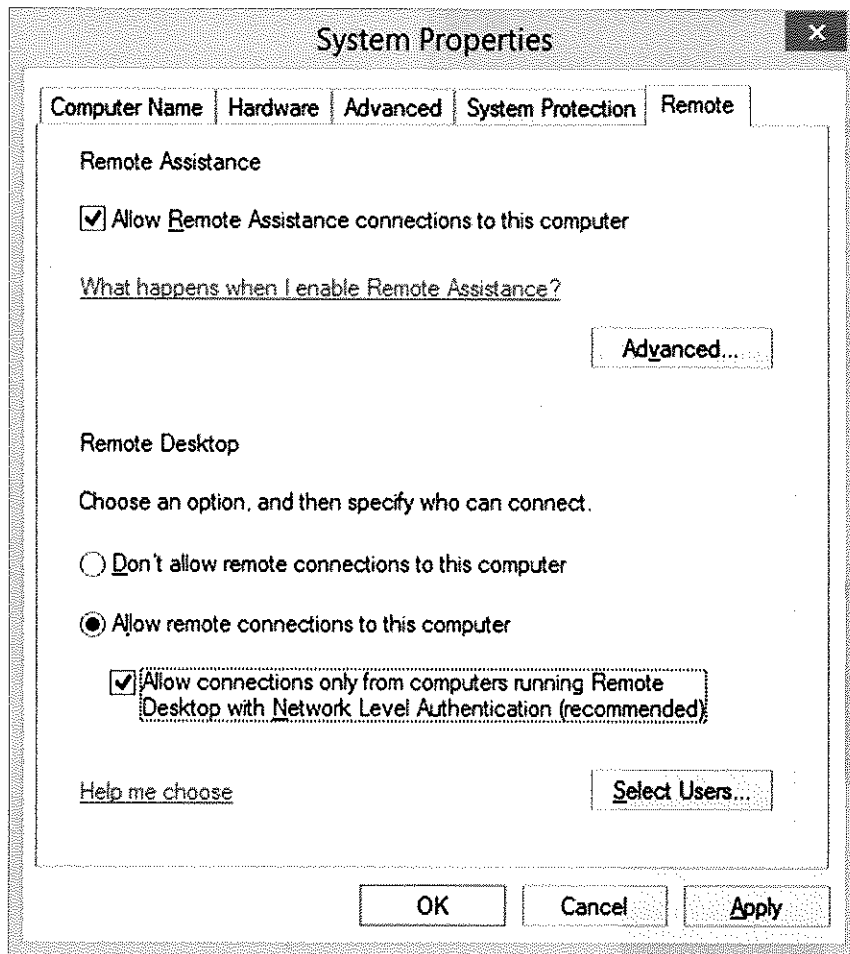




Another way to get to the same menu is to type "This PC" in your Start menu, right click "This PC" and go to Properties:



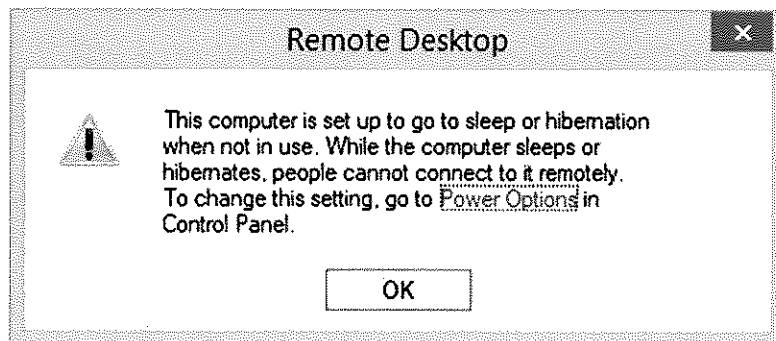
Either way will bring up this menu, where you need to click on the Remote tab:



Select “Allow remote connections to this computer” and the option below it, “Allow connections only from computers running Remote Desktop with Network Level Authentication.”

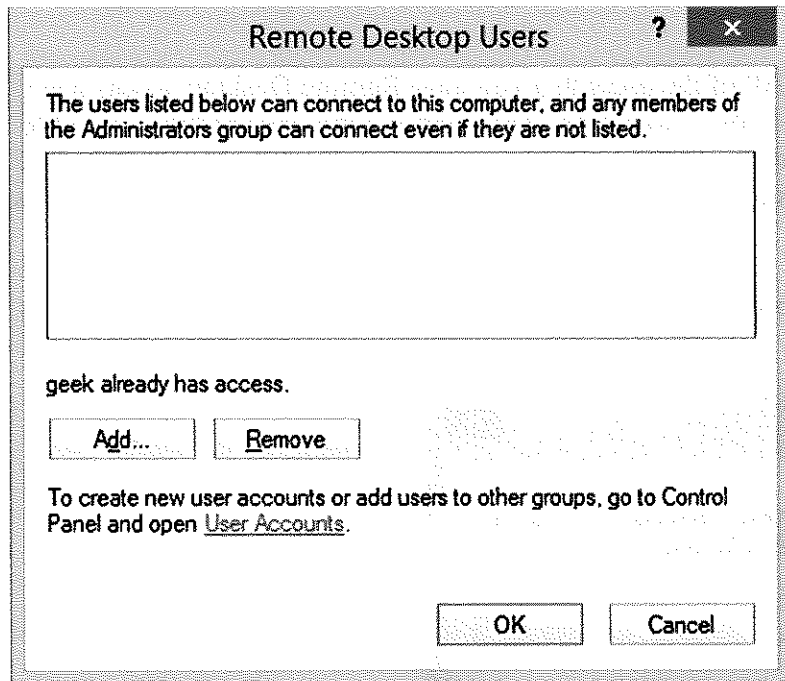
It's not a necessity to require Network Level Authentication, but doing so makes your computer more secure by protecting you from Man in the Middle attacks. Systems even as old as Windows XP can connect to hosts with Network Level Authentication, so there's no reason not to use it.

You may get a warning about your power options when you enable Remote Desktop:

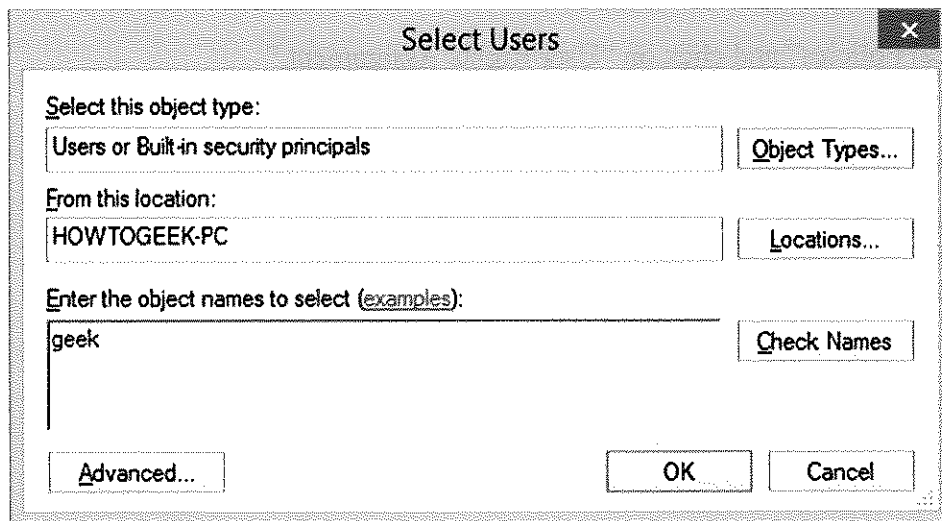


If so, make sure you click the link to Power Options and configure your computer so it doesn't fall asleep or hibernate. See our article on [managing power settings](#) if you need help.

Next, click "Select Users."



Any accounts in the Administrators group will already have access. If you need to grant Remote Desktop access to any other users, just click "Add" and type in the usernames.



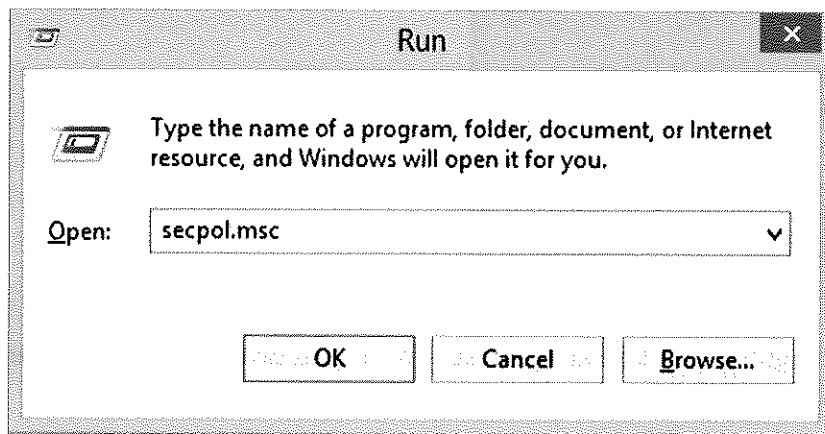
Click "Check Names" to verify the username is typed correctly and then click OK. Click OK on the System Properties window as well.

# Securing Remote Desktop

Your computer is currently connectable via Remote Desktop (only on your local network if you're behind a router), but there are some more settings we need to configure in order to achieve maximum security.

First, let's address the obvious one. All of the users that you gave Remote Desktop access need to have strong passwords. There are a lot of bots constantly scanning the internet for vulnerable PCs running Remote Desktop, so don't underestimate the importance of a strong password. Use more than eight characters (12+ is recommended) with numbers, lowercase and uppercase letters, and special characters.

Go to the Start menu or open a Run prompt (Windows Key + R) and type "secpol.msc" to open the Local Security Policy menu.



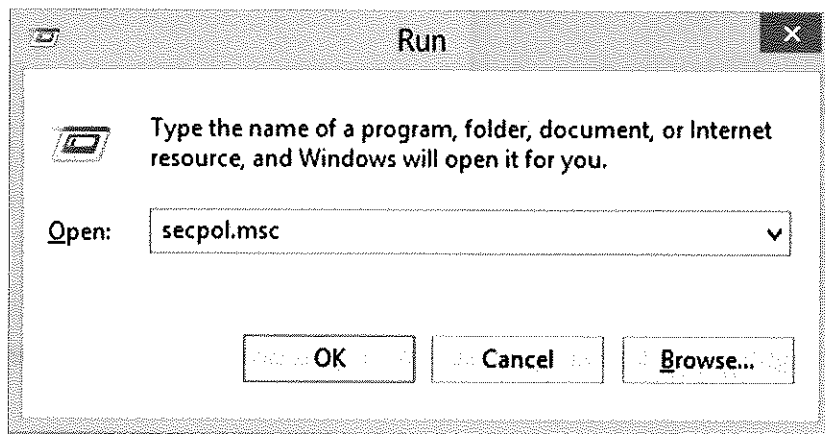
Once there, expand "Local Policies" and click on "User Rights Assignment."

# Securing Remote Desktop

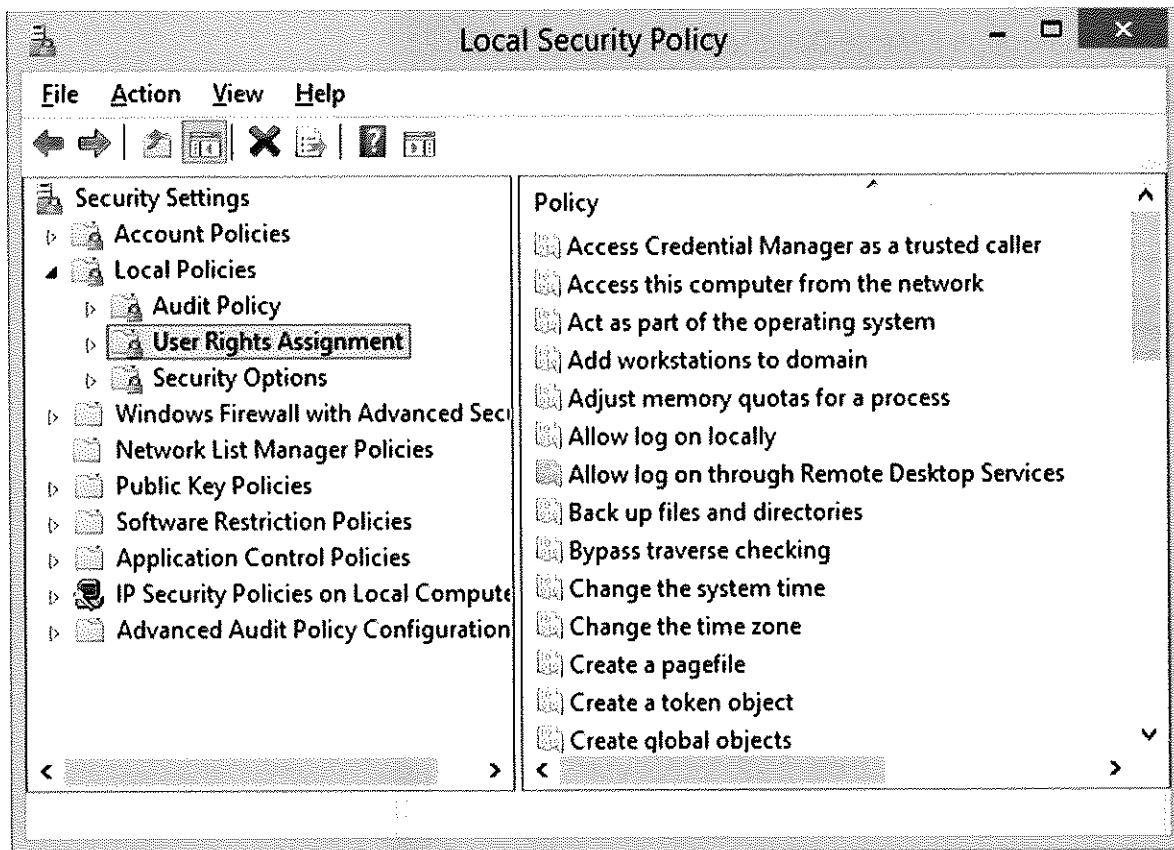
Your computer is currently connectable via Remote Desktop (only on your local network if you're behind a router), but there are some more settings we need to configure in order to achieve maximum security.

First, let's address the obvious one. All of the users that you gave Remote Desktop access need to have strong passwords. There are a lot of bots constantly scanning the internet for vulnerable PCs running Remote Desktop, so don't underestimate the importance of a strong password. Use more than eight characters (12+ is recommended) with numbers, lowercase and uppercase letters, and special characters.

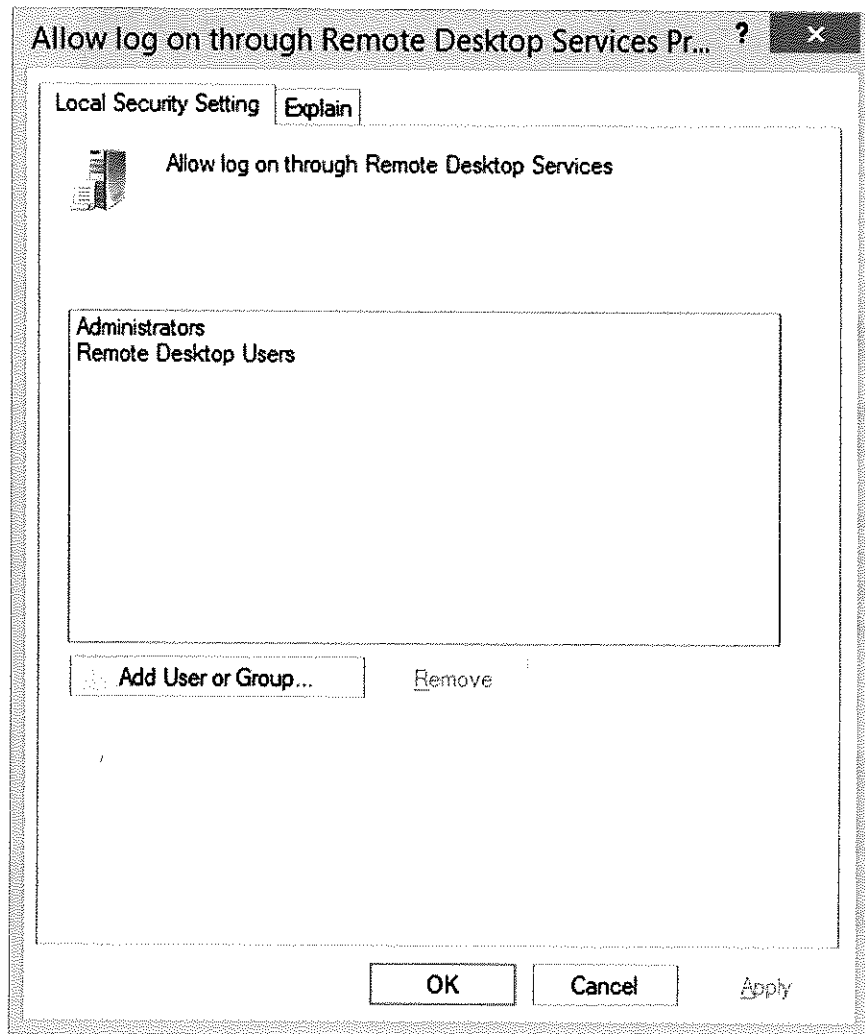
Go to the Start menu or open a Run prompt (Windows Key + R) and type "secpol.msc" to open the Local Security Policy menu.



Once there, expand "Local Policies" and click on "User Rights Assignment."

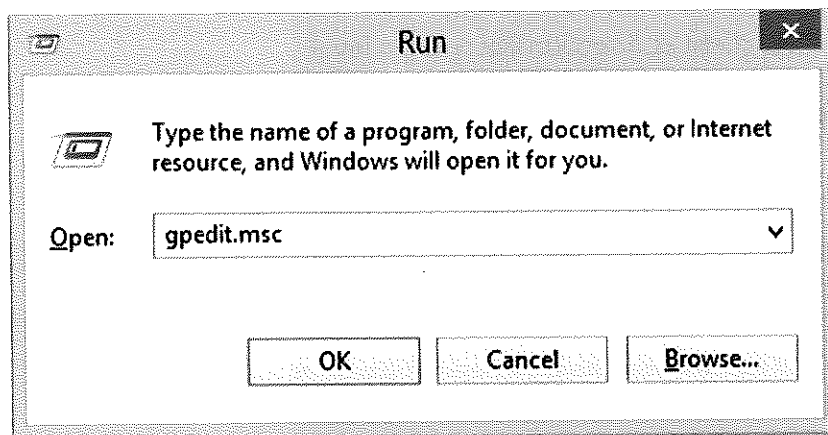


Double-click on the “Allow log on through Remote Desktop Services” policy listed on the right.

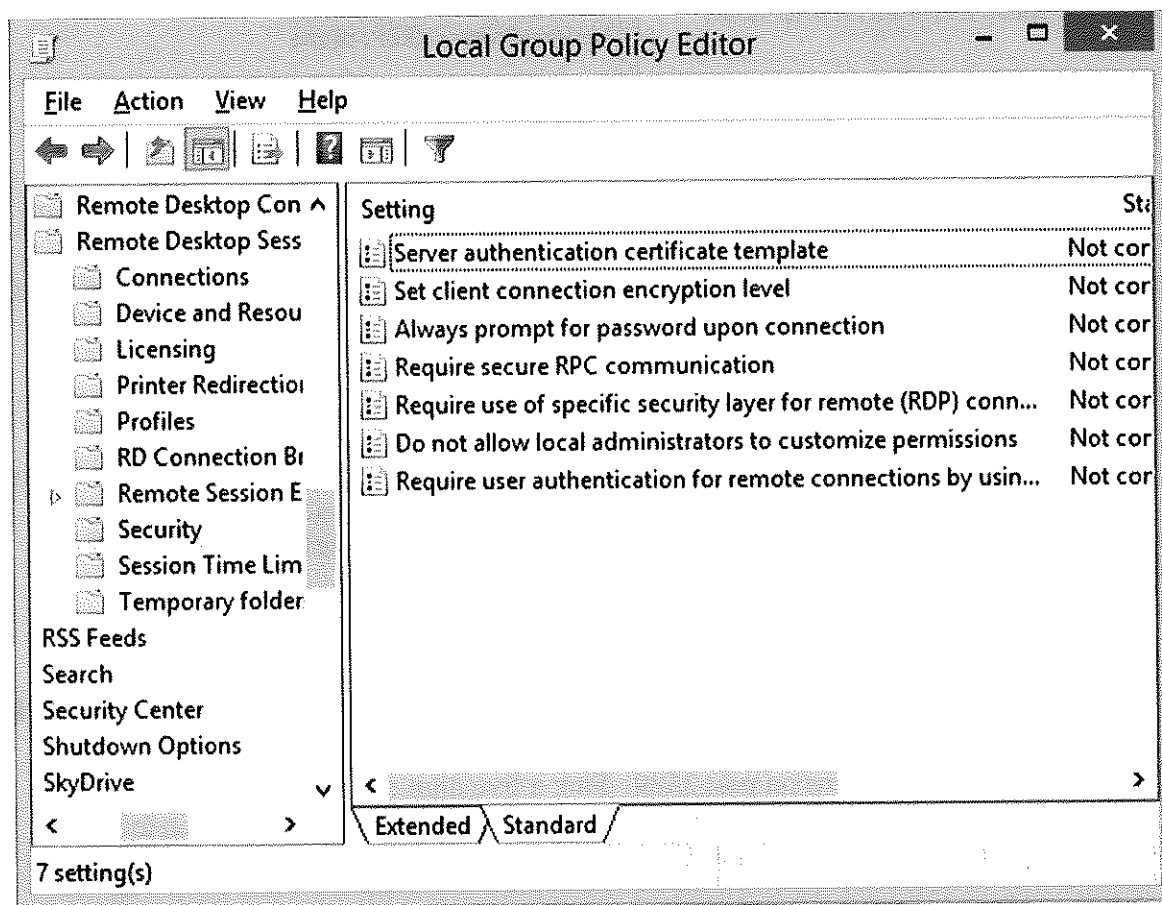


It's our recommendation to remove both of the groups already listed in this window, Administrators and Remote Desktop Users. After that, click "Add User or Group" and manually add the users you'd like to grant Remote Desktop access to. This isn't an essential step, but it gives you more power over which accounts get to use Remote Desktop. If, in the future, you make a new Administrator account for some reason and forget to put a strong password on it, you're opening your computer up to hackers around the world if you never bothered removing the "Administrators" group from this screen.

Close the Local Security Policy window and open the Local Group Policy Editor by typing "gpedit.msc" into either a Run prompt or the Start menu.



When the Local Group Policy Editor opens, expand Computer Policy > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host, and then click on Security.



Double-click on any settings in this menu to change their values. The ones we recommend changing are:

Set client connection encryption level – Set this to High Level so your Remote Desktop sessions are secured with 128-bit encryption.



**Set client connection encryption level**

Set client connection encryption level Previous Setting

☐ Not Configured    Comment:

☒ Enabled

☐ Disabled

Supported on: At least Windows Server 2003 operating systems

Options: Encryption Level: High Level Choose the encryption level from the drop-down list.

Help: This policy setting specifies wh specific encryption level to sec client computers and RD Sess Desktop Protocol (RDP) conne

Require secure RPC communication – Set this to Enabled.

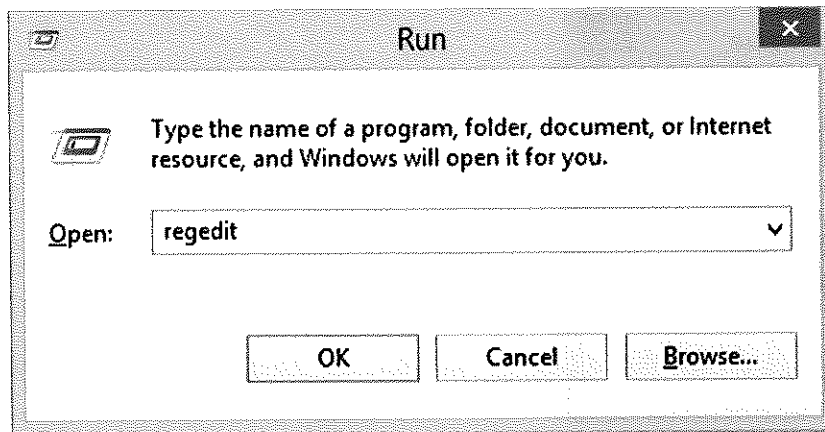
Require use of specific security layer for remote (RDP) connections – Set this to SSL (TLS 1.0).

Require user authentication for remote connections by using Network Level Authentication – Set this to Enabled.

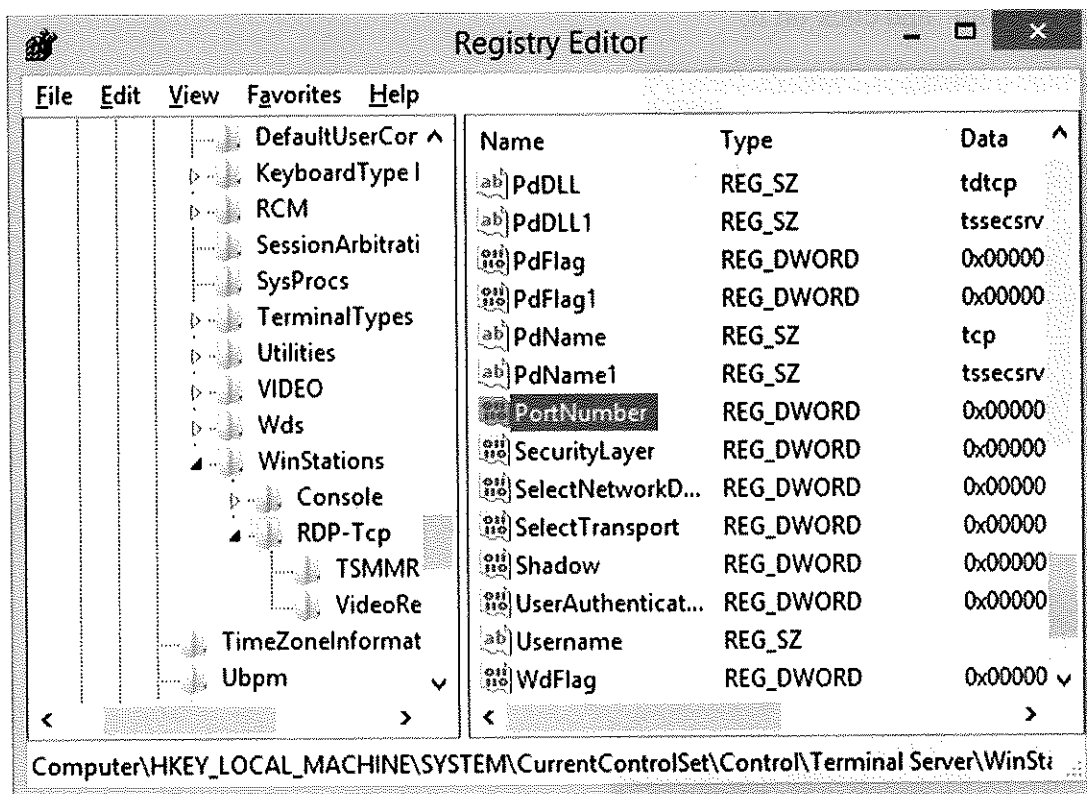
Once those changes have been made, you can close the Local Group Policy Editor. The last security recommendation we have is to change the default port that Remote Desktop listens on. This is an optional step and is considered a security through obscurity practice, but the fact is that changing the default port number greatly decreases the amount of malicious connection attempts that your computer will receive. Your password and security settings need to make Remote Desktop invulnerable no matter what port it is listening on, but we might as well decrease the amount of connection attempts if we can.

## Security through Obscurity: Changing the Default RDP Port

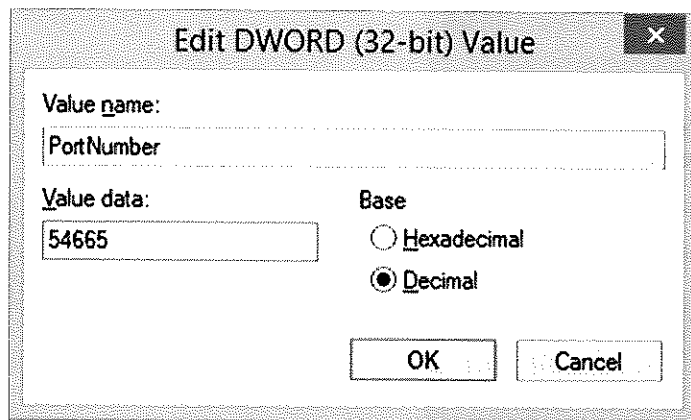
By default, Remote Desktop listens on port 3389. Pick a five digit number less than 65535 that you'd like to use for your custom Remote Desktop port number. With that number in mind, open up the Registry Editor by typing "regedit" into a Run prompt or the Start menu.



When the Registry Editor opens up, expand HKEY\_LOCAL\_MACHINE > SYSTEM > CurrentControlSet > Control > Terminal Server > WinStations > RDP-Tcp > then double-click on "PortNumber" in the window on the right.



With the PortNumber registry key open, select "Decimal" on the right side of the window and then type your five digit number under "Value data" on the left.

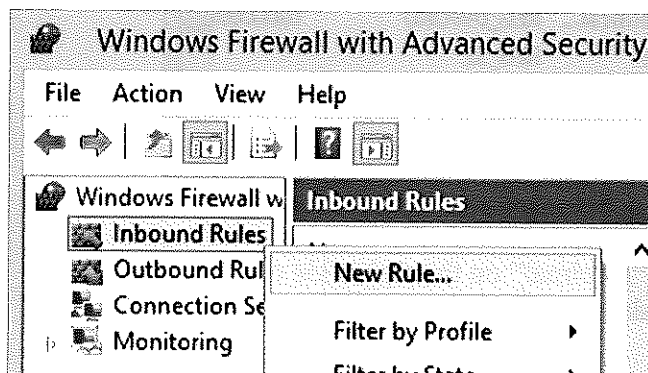


Click OK and then close the Registry Editor.

Since we've changed the default port that Remote Desktop uses, we'll need to configure Windows Firewall to accept incoming connections on that port. Go to the Start screen, search for "Windows Firewall" and click on it.

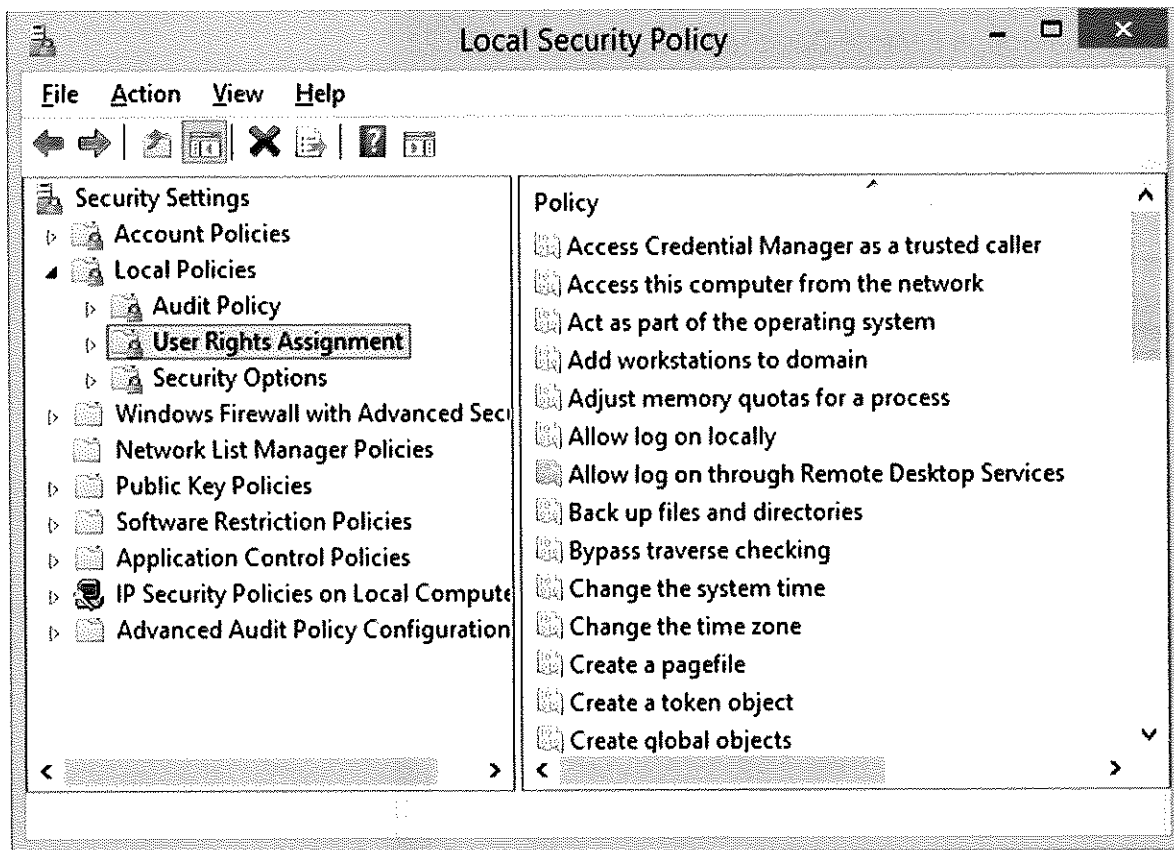


When Windows Firewall opens, click "Advanced Settings" on the left side of the window. Then right-click on "Inbound Rules" and choose "New Rule."

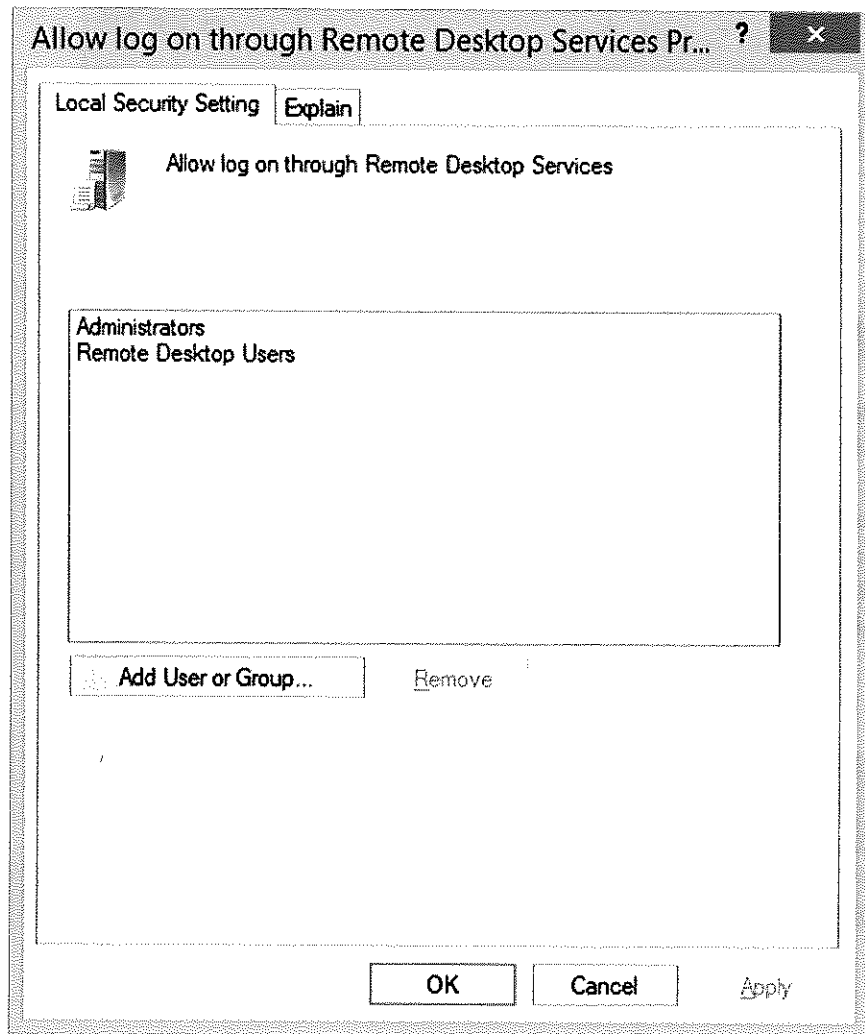


The "New Inbound Rule Wizard" will pop up, select Port and click next. On the next screen, make sure TCP is selected and then enter the port number you chose earlier, and then click next. Click next two more times because the default values on the next couple pages will be

fine. On the last page, select a name for this new rule, such as “Custom RDP port,” and then click finish.

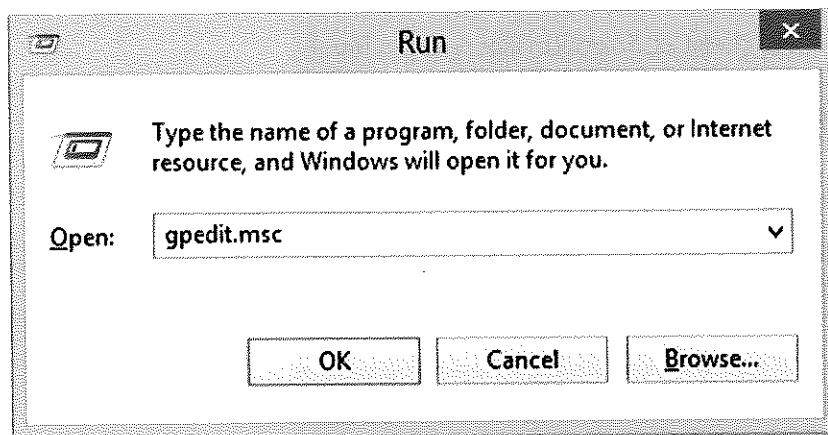


Double-click on the “Allow log on through Remote Desktop Services” policy listed on the right.

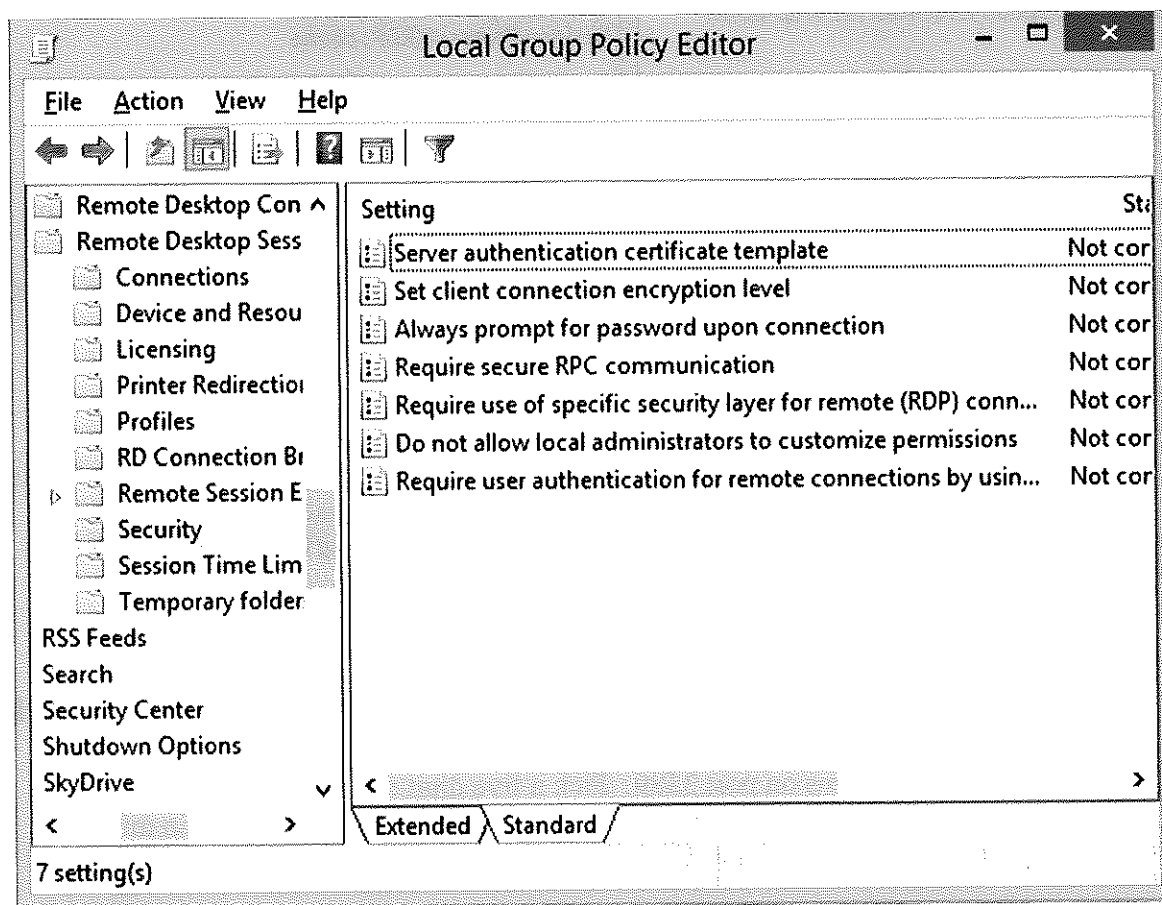


It's our recommendation to remove both of the groups already listed in this window, Administrators and Remote Desktop Users. After that, click "Add User or Group" and manually add the users you'd like to grant Remote Desktop access to. This isn't an essential step, but it gives you more power over which accounts get to use Remote Desktop. If, in the future, you make a new Administrator account for some reason and forget to put a strong password on it, you're opening your computer up to hackers around the world if you never bothered removing the "Administrators" group from this screen.

Close the Local Security Policy window and open the Local Group Policy Editor by typing "gpedit.msc" into either a Run prompt or the Start menu.



When the Local Group Policy Editor opens, expand Computer Policy > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host, and then click on Security.



Double-click on any settings in this menu to change their values. The ones we recommend changing are:

Set client connection encryption level – Set this to High Level so your Remote Desktop sessions are secured with 128-bit encryption.

**Set client connection encryption level**

Set client connection encryption level Previous Setting

☐ Not Configured
 ☒ Enabled
 ☐ Disabled

Comment:

Supported on: At least Windows Server 2003 operating systems

Options: Help:

Encryption Level: High Level ▼

Choose the encryption level from the drop-down list.

This policy setting specifies wh specific encryption level to sec client computerss and RD Sess Desktop Protocol (RDP) conne

Require secure RPC communication – Set this to Enabled.

Require use of specific security layer for remote (RDP) connections – Set this to SSL (TLS 1.0).

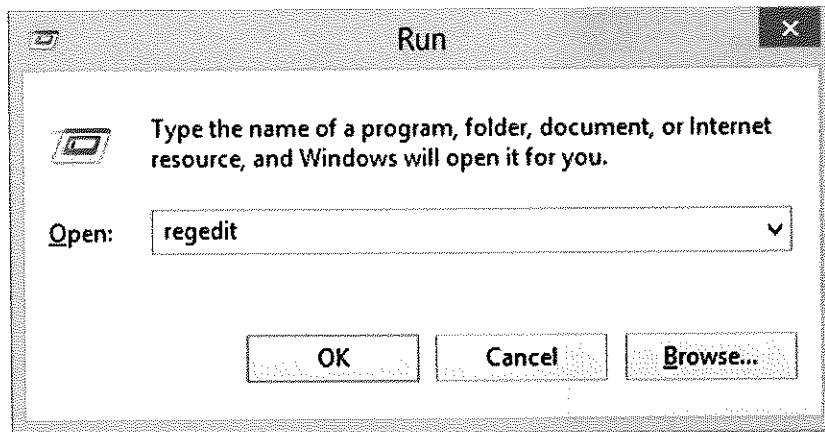
Require user authentication for remote connections by using Network Level Authentication – Set this to Enabled.

Once those changes have been made, you can close the Local Group Policy Editor. The last security recommendation we have is to change the default port that Remote Desktop listens on. This is an optional step and is considered a security through obscurity practice, but the fact is that changing the default port number greatly decreases the amount of malicious connection attempts that your computer will receive. Your password and security settings need to make Remote Desktop invulnerable no matter what port it is listening on, but we might as well decrease the amount of connection attempts if we can.

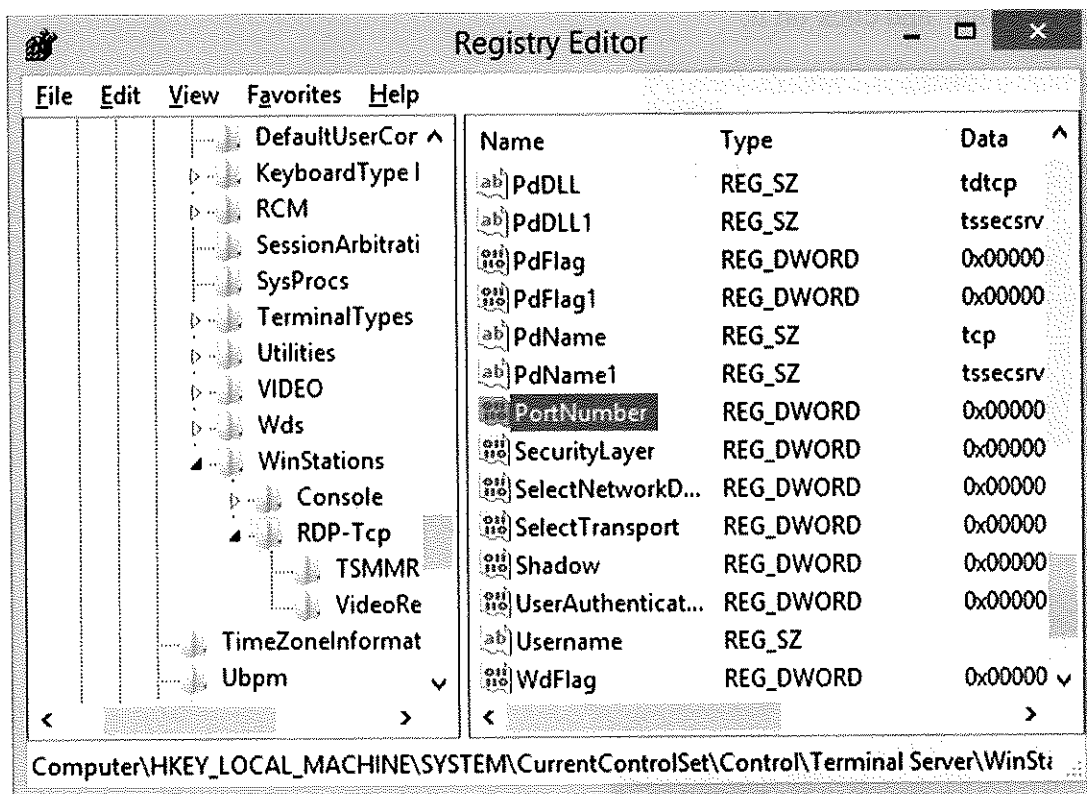
## Security through Obscurity: Changing the Default RDP Port

By default, Remote Desktop listens on port 3389. Pick a five digit number less than 65535 that you'd like to use for your custom Remote Desktop port number. With that number in mind, open up the Registry Editor by typing "regedit" into a Run prompt or the Start menu.

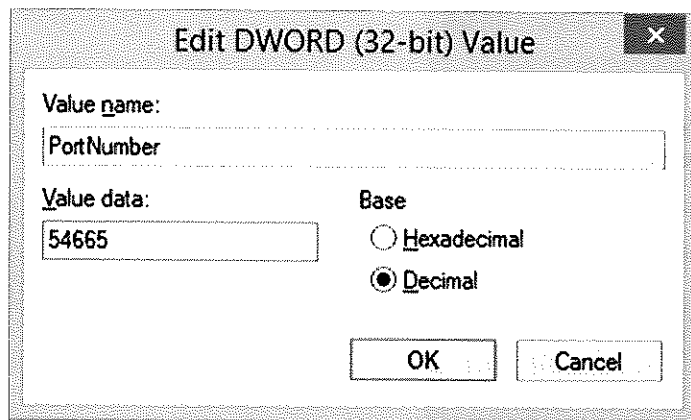




When the Registry Editor opens up, expand HKEY\_LOCAL\_MACHINE > SYSTEM > CurrentControlSet > Control > Terminal Server > WinStations > RDP-Tcp > then double-click on "PortNumber" in the window on the right.



With the PortNumber registry key open, select "Decimal" on the right side of the window and then type your five digit number under "Value data" on the left.

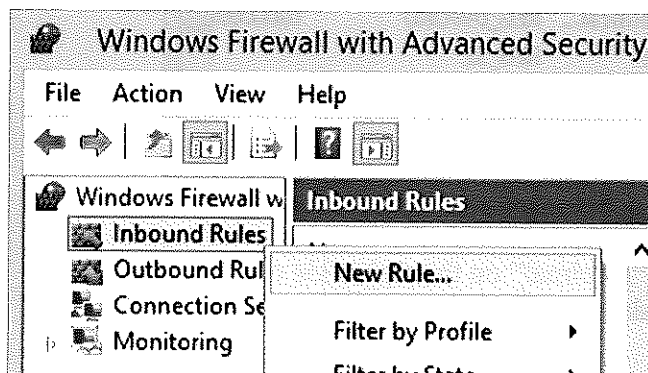


Click OK and then close the Registry Editor.

Since we've changed the default port that Remote Desktop uses, we'll need to configure Windows Firewall to accept incoming connections on that port. Go to the Start screen, search for "Windows Firewall" and click on it.



When Windows Firewall opens, click "Advanced Settings" on the left side of the window. Then right-click on "Inbound Rules" and choose "New Rule."



The "New Inbound Rule Wizard" will pop up, select Port and click next. On the next screen, make sure TCP is selected and then enter the port number you chose earlier, and then click next. Click next two more times because the default values on the next couple pages will be

fine. On the last page, select a name for this new rule, such as “Custom RDP port,” and then click finish.

# Servers

- Part of the Client – Server model
- Make use of ports
- Well known server types:
  - Web Server
  - Mail Server
  - DNS Server
  - Active Directory Server
  - Print Server

# Servers

- Part of the Client – Server model
- Make use of ports
- Well known server types:
  - Web Server
  - Mail Server
  - DNS Server
  - Active Directory Server
  - Print Server

## Web Server

- Everyone knows a web server
- Traditionally run on port 80 and 443  
(Though there are others on different ports)
- Use a web browser to connect to web servers

- IIS → Microsoft

- Apache → linux or windows

## DNS Server

- Routing for the web – like a phone book
- Traditionally run on port 53 (tcp)
- Two types of DNS servers:
  - BIND (unix)
  - Windows DNS (Windows)

## Active Directory (AD) Server

- Corporations use to house user information and corporate rules
- Traditionally run on many ports
- Run on Windows Only



## Print Server

- Used to route print jobs in a LAN environment
- Traditionally run on port 515
- Can be run on Windows and linux

# Modify Zone Transfer Settings

Applies To: Windows Server 2008 R2

You can use the following procedure to control whether a zone will be transferred to other servers and which servers can receive the zone transfer.

Membership in the **Administrators** group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at <http://go.microsoft.com/fwlink/?LinkId=83477>.

## Modifying zone transfer settings

- Using the Windows interface
- Using a command line

*- Secure cache against pollution - easy one*

### To modify zone transfer settings using the Windows interface

1. Open DNS Manager.
2. Right-click a DNS zone, and then click **Properties**.
3. On the **Zone Transfers** tab, do one of the following:
  - To disable zone transfers, clear the **Allow zone transfers** check box.
  - To allow zone transfers, select the **Allow zone transfers** check box.
4. If you allowed zone transfers, do one of the following:
  - To allow zone transfers to any server, click **To any server**.
  - To allow zone transfers only to the DNS servers that are listed on the **Name Servers** tab, click **Only to servers listed on the Name Servers tab**.
  - To allow zone transfers only to specific DNS servers, click **Only to the following servers**, and then add the IP address of one or more DNS servers.

### Additional considerations

- To open DNS Manager, click **Start**, point to **Administrative Tools**, and then click **DNS**.
- To improve the security of your DNS infrastructure, allow zone transfers only for either the DNS servers in the name server (NS) resource records for a zone or for specified DNS servers. If you allow any DNS server to perform a zone transfer, you are allowing internal network information to be transferred to any host that can contact your DNS server.

**To modify zone transfer settings using a command line**

1. Open a command prompt.
2. Type the following command, and then press ENTER:

```
dnscmd <ServerName> /ZoneResetSecondaries <ZoneName> {/NoXfr | /NonSecure | /SecureNs | /SecureList [<SecondaryIPAddress...>]}
```

Parameter	Description
dnscmd	The command-line tool for managing DNS servers.
<ServerName>	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
<ZoneName>	Required. Specifies the fully qualified domain name (FQDN) of the zone.
/NoXfr	Disables zone transfers for the zone.
/NonSecure	Permits zone transfers to any DNS server.
/SecureNs	Permits zone transfers only to DNS servers that are listed in the zone using name server (NS) resource records.
/SecureList	Permits zone transfers only to DNS servers that are specified by <i>SecondaryIPAddress</i> .
<SecondaryIPAddress>	Required, if <b>/SecureList</b> is specified. A list of one or more IP addresses for DNS servers that are permitted to obtain zone transfers.

To view the complete syntax for this command, at a command prompt, type the following command, and then press ENTER:

```
dnscmd /ZoneResetSecondaries /?
```

**Additional considerations**

- To open an elevated Command Prompt window, click **Start**, point to **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
- To improve the security of your DNS infrastructure, allow zone transfers only for either the DNS servers in the

name server NS resource records for a zone or for specified DNS servers. If you allow any DNS server to perform a zone transfer, you are allowing internal network information to be transferred to any host that can contact your DNS server.

### Additional references

- Security Information for DNS

## Community Additions

© 2017 Microsoft

## Web Server

- Everyone knows a web server
- Traditionally run on port 80 and 443

(Though there are others on different ports)

- Use a web browser to connect to web servers

- IIS → Microsoft

- Apache → linux or windows

## Mail Server

- Receives mail from other servers, stores for clients
- Traditionally run on port 25
- In enterprises, use a client like Outlook  
(Many webmail clients like gmail, yahoo, etc. – these also are web servers.)

## DNS Server

- Routing for the web – like a phone book
- Traditionally run on port 53 (tcp)
- Two types of DNS servers:
  - BIND (unix)
  - Windows DNS (Windows)

## Active Directory (AD) Server

- Corporations use to house user information and corporate rules
- Traditionally run on many ports
- Run on Windows Only



## Print Server

- Used to route print jobs in a LAN environment
- Traditionally run on port 515
- Can be run on Windows and linux

# Modify Zone Transfer Settings

Applies To: Windows Server 2008 R2

You can use the following procedure to control whether a zone will be transferred to other servers and which servers can receive the zone transfer.

Membership in the **Administrators** group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at <http://go.microsoft.com/fwlink/?LinkId=83477>.

## Modifying zone transfer settings

- Using the Windows interface
- Using a command line

*- Secure cache against pollution - easy one*

### To modify zone transfer settings using the Windows interface

1. Open DNS Manager.
2. Right-click a DNS zone, and then click **Properties**.
3. On the **Zone Transfers** tab, do one of the following:
  - To disable zone transfers, clear the **Allow zone transfers** check box.
  - To allow zone transfers, select the **Allow zone transfers** check box.
4. If you allowed zone transfers, do one of the following:
  - To allow zone transfers to any server, click **To any server**.
  - To allow zone transfers only to the DNS servers that are listed on the **Name Servers** tab, click **Only to servers listed on the Name Servers tab**.
  - To allow zone transfers only to specific DNS servers, click **Only to the following servers**, and then add the IP address of one or more DNS servers.

### Additional considerations

- To open DNS Manager, click **Start**, point to **Administrative Tools**, and then click **DNS**.
- To improve the security of your DNS infrastructure, allow zone transfers only for either the DNS servers in the name server (NS) resource records for a zone or for specified DNS servers. If you allow any DNS server to perform a zone transfer, you are allowing internal network information to be transferred to any host that can contact your DNS server.

**To modify zone transfer settings using a command line**

1. Open a command prompt.
2. Type the following command, and then press ENTER:

```
dnscmd <ServerName> /ZoneResetSecondaries <ZoneName> {/NoXfr | /NonSecure | /SecureNs | /SecureList [<SecondaryIPAddress...>]}
```

Parameter	Description
dnscmd	The command-line tool for managing DNS servers.
<ServerName>	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
<ZoneName>	Required. Specifies the fully qualified domain name (FQDN) of the zone.
/NoXfr	Disables zone transfers for the zone.
/NonSecure	Permits zone transfers to any DNS server.
/SecureNs	Permits zone transfers only to DNS servers that are listed in the zone using name server (NS) resource records.
/SecureList	Permits zone transfers only to DNS servers that are specified by <i>SecondaryIPAddress</i> .
<SecondaryIPAddress>	Required, if <b>/SecureList</b> is specified. A list of one or more IP addresses for DNS servers that are permitted to obtain zone transfers.

To view the complete syntax for this command, at a command prompt, type the following command, and then press ENTER:

```
dnscmd /ZoneResetSecondaries /?
```

**Additional considerations**

- To open an elevated Command Prompt window, click **Start**, point to **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
- To improve the security of your DNS infrastructure, allow zone transfers only for either the DNS servers in the

name server NS resource records for a zone or for specified DNS servers. If you allow any DNS server to perform a zone transfer, you are allowing internal network information to be transferred to any host that can contact your DNS server.

### Additional references

- Security Information for DNS

## Community Additions

© 2017 Microsoft

# Restrict a DNS server to listen only on selected addresses

Applies To: Windows Server 2008 R2

By default, a DNS Server service that is running on a multihomed computer is configured to listen for DNS queries using all of its IP addresses. You can make the DNS server more secure by limiting the IP addresses that the DNS Server service listens on to the IP address that is used by its DNS clients as their preferred DNS server.

Membership in the **Administrators** group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at <http://go.microsoft.com/fwlink/?LinkId=83477>.

## Restricting a DNS server to listen only on selected addresses

- Using the Windows interface
- Using a command line

### To restrict a DNS server to listen only on selected addresses using the Windows interface

1. Open DNS Manager.
2. In the console tree, click the applicable DNS server.

#### Where?

- DNS/*applicable DNS server*

3. On the **Action** menu, click **Properties**.
4. On the **Interfaces** tab, click **Only the following IP addresses**.
5. In **IP address**, type an IP address to be enabled for this DNS server, and then click **Add**.
6. Repeat the previous step as necessary to specify other server IP addresses to be enabled for this DNS server.

To remove an IP address from the list, click it, and then click **Remove**.

### Additional considerations

- To open DNS Manager, click **Start**, point to **Administrative Tools**, and then click **DNS**.
- By default, the DNS Server service listens for DNS message communications on all configured IP addresses for the server computer.
- Server IP addresses that are added here must be managed statically. If you later change or remove the addresses specified here from the TCP/IP configurations that are maintained at this server, update this list accordingly.

- After you update or revise the list of restricted interfaces, you must stop and restart the DNS server to apply the new list.
- Restricting the DNS Server service to only listen on specific IP addresses is an effective security measure because only hosts on the same network subnet, or hosts with a router that connects them to that same segment, have access to the server.

**To restrict a DNS server to listen only on selected addresses using a command line**

1. Open a command prompt.
2. Type the following command, and then press ENTER:

```
dnscmd <ServerName> /ResetListenAddresses [<ListenAddress> ...]
```

Parameter	Description
dnscmd	Specifies the name of the command-line tool for managing DNS servers.
<ServerName>	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
/ResetListenAddresses	Required. Resets the IP addresses of the interfaces on which the DNS server listens.
<ListenAddress> ...	Specifies one or more IP addresses for the interfaces on which you want the DNS server to listen. By default, the DNS Server service listens for DNS message communications on all configured IP addresses for the server computer.

To view the complete syntax for this command, at a command prompt, type the following command, and then press ENTER:

```
dnscmd <ServerName> /ResetListenAddresses /help
```

**Additonal considerations**

- To open an elevated Command Prompt window, click **Start**, point to **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
- Server IP addresses that you add here must be managed statically. If you later change or remove the addresses specified here from the TCP/IP configurations that are maintained at this server, update this list accordingly.

- After you update or revise the list of restricted interfaces, you must stop and restart the DNS server to apply the new list.
- Restricting the DNS Server service to listen only on specific IP addresses is an effective security measure because only hosts on the same network subnet, or hosts with a router that connects them to that same segment, have access to the server.

### Additional references

- Start or Stop a DNS Server
- Configuring Multihomed Servers
- Security Information for DNS
- Securing the DNS Server Service
- Securing DNS Clients

### Community Additions

© 2017 Microsoft

# Secure the Server Cache Against Names Pollution

Applies To: Windows Server 2008 R2

By default, the DNS Server service is secured from cache pollution, which occurs when DNS query responses contain nonauthoritative or malicious data. The **Secure cache against pollution** option prevents an attacker from successfully polluting the cache of a DNS server with resource records that were not requested by the DNS server. Changing this default setting will reduce the integrity of the responses that are provided by DNS Server service. You can use this procedure to restore the default setting if it was previously changed.

Membership in the **Administrators** group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at <http://go.microsoft.com/fwlink/?LinkId=83477>.

## To secure the server cache against names pollution

1. Open DNS Manager.
2. In the console tree, click the applicable DNS server.

### Where?

- DNS/applicable DNS server

3. On the **Action** menu, click **Properties**.
4. Click the **Advanced** tab.
5. In **Server options**, select the **Secure cache against pollution** check box, and then click **OK**.

## Additional considerations

- To open DNS Manager, click **Start**, point to **Administrative Tools**, and then click **DNS**.
- The **Secure cache against pollution** option is enabled by default.

## Additional references

- Security Information for DNS
- Securing the DNS Server Service

## Community Additions



# Allow Only Secure Dynamic Updates

Applies To: Windows Server 2008, Windows Server 2008 R2

Domain Name System (DNS) client computers can use dynamic update to register and dynamically update their resource records with a DNS server whenever changes occur. This reduces the need for manual administration of zone records, especially for clients that frequently move or change locations and use Dynamic Host Configuration Protocol (DHCP) to obtain an IP address.

Dynamic updates can be secure or nonsecure. DNS update security is available only for zones that are integrated into Active Directory Domain Services (AD DS). After you directory-integrate a zone, access control list (ACL) editing features are available in DNS Manager so that you can add or remove users or groups from the ACL for a specified zone or resource record.

Membership in the **Administrators** group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at <http://go.microsoft.com/fwlink/?LinkId=83477>.

## Allowing only secure dynamic updates

- Using the Windows interface
- Using a command line

### To allow only secure dynamic updates using the Windows interface

1. Open DNS Manager.
2. In the console tree, right-click the applicable zone, and then click **Properties**.
3. On the **General** tab, verify that the zone type is **Active Directory-integrated**.
4. In **Dynamic Updates**, click **secure only**.

### Additional considerations

- To open DNS Manager, click **Start**, point to **Administrative Tools**, and then click **DNS**.
- Secure dynamic update is supported only for AD DS-integrated zones. If the zone type is configured differently, you must change the zone type and directory-integrate the zone before securing it for DNS dynamic updates.
- Dynamic update is a Request for Comments (RFC)-compliant extension to the DNS standard. The DNS update process is defined in RFC 2136, "Dynamic Updates in the Domain Name System (DNS UPDATE)."
- By default, the DNS server allows a zone transfer only to authoritative DNS servers that are listed in the name server (NS) resource records for the zone.

### To allow only secure dynamic updates using a command line

1. Open a command prompt.
2. Type the following command, and then press ENTER:

```
dnscmd <ServerName> /Config {<ZoneName>|..AllZones} /AllowUpdate 2
```

Parameter	Description
dnscmd	The command-line tool for managing DNS servers.
<ServerName>	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.)
/Config	Required. Configures the specified zone.
<ZoneName> ..AllZones	Required. Specifies the fully qualified domain name (FQDN) of the zone. To configure all zones that are hosted on the specified DNS server to allow dynamic updates, type <b>..AllZones</b> .
/AllowUpdate	Required. Enables the zone to perform dynamic updates.
2	Required. Configures the server to allow secure update. If you exclude the 2, the zone will be set to perform standard dynamic updates only.

To view the complete syntax for this command, at a command prompt, type the following command, and then press ENTER:

```
dnscmd /Config /help
```

### Additional considerations

- To open an elevated Command Prompt window, click **Start**, point to **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
- Dynamic update is an RFC-compliant extension to the DNS standard. The DNS update process is defined in RFC 2136, "Dynamic Updates in the Domain Name System (DNS UPDATE)."
- By default, the DNS server allows a zone transfer only to authoritative DNS servers that are listed in the name server (NS) resource records for the zone.

# Disable Recursion on the DNS Server

Applies To: Windows Server 2008 R2

By default, the DNS server performs recursive queries on behalf of its DNS clients and DNS servers that have forwarded DNS client queries to it. Recursion is a name-resolution technique in which a DNS server queries other DNS servers on behalf of the requesting client to fully resolve the name and then sends an answer back to the client.

Attackers can use recursion to deny the DNS Server service. Therefore, if a DNS server in your network is not intended to receive recursive queries, recursion should be disabled on that server.

Membership in the **Administrators** group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at <http://go.microsoft.com/fwlink/?LinkId=83477>.

## Disabling recursion on the DNS server

- Using the Windows interface
- Using a command line

### To disable recursion on the DNS server using the Windows interface

1. Open DNS Manager.
2. In the console tree, right-click the applicable DNS server, then click **Properties**.

#### Where?

*DNS/applicable DNS server*

3. Click the **Advanced** tab.
4. In **Server options**, select the **Disable recursion** check box, and then click **OK**.

### Additional considerations

- To open DNS Manager, click **Start**, point to **Administrative Tools**, and then click **DNS**.
- If you disable recursion on the DNS server, you will not be able to use forwarders on the same server.

### To disable recursion on the DNS server using a command line

1. Open a command prompt.
2. Type the following command, and then press ENTER:

```
dnscmd <ServerName> /Config /NoRecursion {1|0}
```

Parameter	Description
dnscmd	Specifies the name of the command-line tool for managing DNS servers.
<ServerName>	Required. Specifies the DNS host name of the DNS server. You can also type the IP address of the DNS server. To specify the DNS server on the local computer, you can also type a period (.).
/Config	Required. Specifies that the command configures the specified server.
/NoRecursion	Required. Disables recursion.
{1 0}	Required. To disable recursion, type <b>1</b> (off). To enable recursion, type <b>0</b> (on). By default, recursion is enabled.

To view the complete syntax for this command, at a command prompt, type the following command, and then press ENTER:

```
dnscmd /Config /help
```

### Additional considerations

- To open an elevated Command Prompt window, click **Start**, point to **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**.
- If you disable recursion on the DNS server, you will not be able to use forwarders on the same server.

### Additional references

- Security Information for DNS
- Securing the DNS Server Service

## Community Additions

# Update Root Hints on the DNS Server

Applies To: Windows Server 2008 R2

You can use root hints to prepare servers that are authoritative for nonroot zones so that they can discover authoritative servers that manage domains at a higher level or in other subtrees of the DNS domain namespace. These root hints are essential for servers that are authoritative at lower levels of the namespace when locating and finding other servers under these conditions.

Membership in the **Administrators** group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at <http://go.microsoft.com/fwlink/?LinkId=83477>.

## To update root hints on the DNS server

1. Open DNS Manager.
2. In the console tree, click the applicable DNS server.

### Where?

- DNS/*applicable DNS server*

3. On the **Action** menu, click **Properties**.
4. Click the **Root Hints** tab.
5. Modify server root hints as follows:

- To add a root server to the list, click **Add**, and then specify the name and IP address of the server to be added to the list.
- To modify a root server in the list, click **Edit**, and then specify the name and IP address of the server to be modified in the list.
- To remove a root server from the list, select it in the list, and then click **Remove**.
- To copy root hints from a DNS server, click **Copy from server**, and then specify the IP address of the DNS server from which you want to copy a list of root servers to use in resolving queries. These root hints will not overwrite any existing root hints.

## Additional considerations

- To open DNS Manager, click **Start**, point to **Administrative Tools**, and then click **DNS**.

## Additional references

- Updating Root Hints
- Security Information for DNS

# Modify Security for the DNS Server Service on a Domain Controller

Applies To: Windows Server 2008 R2

You can use this procedure to specify who can administer the DNS Server service when it is running on a domain controller. It does not affect who can administer zones and resource records that are hosted on the server, however.

Membership in the **Administrators** group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at <http://go.microsoft.com/fwlink/?LinkId=83477>.

## To modify security for the DNS Server service on a domain controller

1. Open DNS Manager.
2. In the console tree, right-click the applicable server, and then click **Properties**.

### Where?

*DNS/applicable DNS server*

3. On the **Security** tab, modify the list of member users or groups that are allowed to administer the applicable server.

## Additional considerations

- To open DNS Manager, click **Start**, point to **Administrative Tools**, and then click **DNS**.
- Active Directory access control lists (ACLs) are supported for the DNS Server service only when it is running on a domain controller.

## Additional references

- [Configure a DNS Server for Use with Active Directory Domain Services](#)
- [Modify Security for a Directory-Integrated Zone](#)
- [Modify Security for a Resource Record](#)

## Community Additions

# Modify Security for the DNS Server Service on a Domain Controller

Applies To: Windows Server 2008 R2

You can use this procedure to specify who can administer the DNS Server service when it is running on a domain controller. It does not affect who can administer zones and resource records that are hosted on the server, however.

Membership in the **Administrators** group, or equivalent, is the minimum required to complete this procedure. Review details about using the appropriate accounts and group memberships at <http://go.microsoft.com/fwlink/?LinkId=83477>.

## To modify security for the DNS Server service on a domain controller

1. Open DNS Manager.
2. In the console tree, right-click the applicable server, and then click **Properties**.

### Where?

*DNS/applicable DNS server*

3. On the **Security** tab, modify the list of member users or groups that are allowed to administer the applicable server.

## Additional considerations

- To open DNS Manager, click **Start**, point to **Administrative Tools**, and then click **DNS**.
- Active Directory access control lists (ACLs) are supported for the DNS Server service only when it is running on a domain controller.

## Additional references

- [Configure a DNS Server for Use with Active Directory Domain Services](#)
- [Modify Security for a Directory-Integrated Zone](#)
- [Modify Security for a Resource Record](#)

## Community Additions