**1. How to enable the password complexity requirement?**

* Passwords may not contain the user's samAccountName (Account Name) value or entire displayName (Full Name value). Both checks aren't case-sensitive.
  + The samAccountName is checked in its entirety only to determine whether it's part of the password. If the samAccountName is fewer than three characters long, this check is skipped. The displayName is parsed for delimiters: commas, periods, dashes or hyphens, underscores, spaces, pound signs, and tabs. If any of these delimiters are found, the displayName is split and all parsed sections (tokens) are confirmed not to be included in the password. Tokens that are shorter than three characters are ignored, and substrings of the tokens aren't checked. For example, the name "Erin M. Hagens" is split into three tokens: "Erin", "M", and "Hagens". Because the second token is only one character long, it's ignored. So, this user could not have a password that included either "erin" or "hagens" as a substring anywhere in the password.
* The password contains characters from three of the following categories:
  + Uppercase letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
  + Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
  + Base 10 digits (0 through 9)
  + Non-alphanumeric characters (special characters): (~!@#$%^&\*\_-+=`|\(){}[]:;"'<>,.?/) Currency symbols such as the Euro or British Pound aren't counted as special characters for this policy setting.
  + Any Unicode character that's categorized as an alphabetic character but isn't uppercase or lowercase. This group includes Unicode characters from Asian languages.

2. How to set the inbound and outbound rules in windows firewall?

* Inbound

1. Open the Group Policy Management Console to [Windows Defender Firewall with Advanced Security](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/open-the-group-policy-management-console-to-windows-firewall-with-advanced-security).
2. In the navigation pane, click **Inbound Rules**.
3. Click **Action**, and then click **New rule**.
4. On the **Rule Type** page of the New Inbound Rule Wizard, click **Custom**, and then click **Next**.  
   **Note:** Although you can create rules by selecting **Program** or **Port**, those choices limit the number of pages presented by the wizard. If you select **Custom**, you see all of the pages, and have the most flexibility in creating your rules.
5. On the **Program** page, click **All programs**, and then click **Next**.  
   **Note:** This type of rule is often combined with a program or service rule. If you combine the rule types, you get a firewall rule that limits traffic to a specified port and allows the traffic only when the specified program is running. The specified program cannot receive network traffic on other ports, and other programs cannot receive network traffic on the specified port. If you choose to do this, follow the steps in the [Create an Inbound Program or Service Rule](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-an-inbound-program-or-service-rule) procedure in addition to the steps in this procedure to create a single rule that filters network traffic using both program and port criteria.
6. On the **Protocol and Ports** page, select the protocol type that you want to allow. To restrict the rule to a specified port number, you must select either **TCP** or **UDP**. Because this is an incoming rule, you typically configure only the local port number.  
   If you select another protocol, then only packets whose protocol field in the IP header match this rule are permitted through the firewall.  
   To select a protocol by its number, select **Custom** from the list, and then type the number in the **Protocol number** box.  
   When you have configured the protocols and ports, click **Next**.
7. On the **Scope** page, you can specify that the rule applies only to network traffic to or from the IP addresses entered on this page. Configure as appropriate for your design, and then click **Next**.
8. On the **Action** page, select **Allow the connection**, and then click **Next**.
9. On the **Profile** page, select the network location types to which this rule applies, and then click **Next**.  
   **Note:** If this GPO is targeted at server computers running Windows Server 2008 that never move, consider modifying the rules to apply to all network location type profiles. This prevents an unexpected change in the applied rules if the network location type changes due to the installation of a new network card or the disconnection of an existing network card’s cable. A disconnected network card is automatically assigned to the Public network location type.
10. On the **Name** page, type a name and description for your rule, and then click **Finish**.

* Outbound

1. Open the Group Policy Management Console to [Windows Defender Firewall with Advanced Security](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/open-the-group-policy-management-console-to-windows-firewall-with-advanced-security).
2. In the navigation pane, click **Outbound Rules**.
3. Click **Action**, and then click **New rule**.
4. On the **Rule Type** page of the New Outbound Rule wizard, click **Custom**, and then click **Next**.  
   **Note:** Although you can create rules by selecting **Program** or **Port**, those choices limit the number of pages presented by the wizard. If you select **Custom**, you see all of the pages, and have the most flexibility in creating your rules.
5. On the **Program** page, click **All programs**, and then click **Next**.
6. On the **Protocol and Ports** page, select the protocol type that you want to block. To restrict the rule to a specified port number, you must select either **TCP** or **UDP**. Because this is an outbound rule, you typically configure only the remote port number.  
   If you select another protocol, then only packets whose protocol field in the IP header match this rule are blocked by Windows Defender Firewall. Network traffic for protocols is allowed as long as other rules that match do not block it.  
   To select a protocol by its number, select **Custom** from the list, and then type the number in the **Protocol number** box.  
   When you have configured the protocols and ports, click **Next**.
7. On the **Scope** page, you can specify that the rule applies only to network traffic to or from the IP addresses entered on this page. Configure as appropriate for your design, and then click **Next**.
8. On the **Action** page, select **Block the connection**, and then click **Next**.
9. On the **Profile** page, select the network location types to which this rule applies, and then click **Next**.
10. On the **Name** page, type a name and description for your rule, and then click **Finish**.

3. How to apply the IP security?

Setting up the IP Policy

1. Log into your dedicated server using **Remote Desktop**.
2. Click **Start > Run >**type **MMC** press **OK**.
3. In the console click **File > Add/Remove Snap in**.
4. Select the **IP Security Policy Managment** item in the **Available snap-ins** list click the Add button.
5. Leave **Local Computer** checked and click **Finish** and then **OK.** You should now be back to the console.
6. If no Security Policy exists yet, in the Left frame right click **IP Security Policies on Local Computer** and then click **Create IP Security Policy** then continue to next step**.** If a Security Policy does exist, right click on it in the Right pane and click Properties then continue to next section (Setting up the IP Filters)
7. Click **Next** on the first page of the Wizard
8. Name your IP Security Policy and provide a description if desired, then click **Next**.
9. Check the box for the **Activate the default response rule** option then click **Next**.
10. Leave the **Active Directory default** option on the **Default Response Rule Authentication Method** page selected and click **Next**.
11. On the final page of the Wizard leave the **Edit properties** option checked and click **Finish**. You should now have the properties window open.

Setting up the IP Filters to ALLOW access

**These steps must be completed to allow access to your server from the Managed.com subnets to allow administration of the server by Managed.com Support technicians and our access by our optimization tools. You will also need to allow any IP addresses you want to use to access your server.**

**Managed.com Subnets:**

**US: 208.88.72.0/21 and 70.34.32.0/20**

**UK: 212.84.80.0/22**

**EU 1:70.34.40.0/21**

**AU: 199.241.152.0/21**

1. Click **Add** then click **Next** to continue.
2. Leave **This rule does not specify a tunnel** selected and click **Next**.
3. Leave **all network connections** selected and click **Next**.
4. You should now be on the IP filter list. You need to create a new filter, so don't select any of the default ones. Click **Add**.
5. Type a Name for your list, and a Description if desired.
6. Leave **Mirrored. Match packets with the exact opposite source and destination addresses** checked. Click **Next**.
7. Select **A specific IP Address of Subnet** as the **Source address,** enter the IP of Subnet you want to allow (see note above for Managed.com subnets) then click **Next.**
8. You can now select **A Specific IP Address** or **Any IP Address** for the Destination address.
9. Select the **Protocol Type** you wish to allow access to. Click Next and then Finish.
10. Complete the steps above for each additional IP address you want to add to the Filter.
11. Once you have added all the required IP Addresses to the list click **OK**.
12. Select the list you have just created from the IP Filter List and click **Next**.
13. In the **Filter Action** box click **Add** to create a new Action for the List you've selected.
14. Click **Next** on the first page of the Filter Action Wizard
15. Give your action a name such as AllowConnection and click **Next**.
16. Select the **Permit** radio button and click **Next**.
17. Click **Finish**.
18. Select the Filter Action you've just created and click **Next** then **Finish**.
19. Click **OK** to close the RDP Policy Properties box.

Once you have added the filter to ALLOW access, follow the steps block unwanted access to the server or particular protocols.

Setting up the IP Filters to BLOCK access

**Using Any IP Address as the IP Traffic Source will block access from all sources and is not recommended unless blocking access to a single protocol such as RDP, you will first need to complete the steps above to allow access to the Managed.com subnet, and any other IP addresses you wish to allow access to your server.**

1. Click **Add** then click **Next** to continue.
2. Leave **This rule does not specify a tunnel** selected and click **Next**.
3. Leave **all network connections** selected and click **Next**.
4. You should now be on the IP filter list. You need to create a new filter, so don't select any of the default ones. Click **Add**.
5. Type a Name for your list, and a Description if desired.
6. Click **Add...** then click **Next** to continue.
7. In the description box type a description.
8. Leave **Mirrored. Match packets with the exact opposite source and destination addresses** checked. Click **Next**.
9. Select the Source of the traffic you with to block then click **Next**.
10. You can now select **A Specific IP Address** or **Any IP Address** for the Destination address.
11. If you have selected **A specific IP Address**, type in the IP Address you want to block. Click **Next**.
12. Select the **Protocol Type** you wish to block, or select **Any** if you want to block access to all protocols. Next and then Finish.
13. Complete the steps above for each additional IP address you want to add to the Filter list, or if you have blocked all IP addresses continue to the next step.
14. Once you have added all the required IP Addresses to the list click **OK**.
15. Select the list you have just created from the IP Filter List and click **Next**.
16. In the **Filter Action** box select the **BlockConnection** option and click Next.
17. Click **Finish**.
18. Click **OK** to close the RDP Policy Properties box.
19. Once you're back in the Console/IP Security Policies screen, right click on the Policy you have just created and select Assign. This step will not be necessary if you are using an existing Policy.

4. How to apply the encryption?

File encryption helps protect your data by encrypting it. Only someone with the right encryption key (such as a password) can decrypt it. File encryption is not available in Windows 10 Home.

1. Right-click (or press and hold) a file or folder and select **Properties**.
2. Select the **Advanced** button and select the **Encrypt contents to secure data** check box.
3. Select **OK** to close the **Advanced Attributes** window, select **Apply**, and then select **OK**.

5. How to apply the security on the folder, full access for simple users?

* Setting permissions

Once you have granted a group or individual user access to a folder, you will need to set permissions for the new user(s). When you set permissions, you are specifying what level of access a user(s) has to the folder and the files within it. Be careful about checking *Deny* for any permissions, as the *Deny* permission overrides any other related to *Allow* permissions.

Folder permissions can be changed only by the owner of the folder (i.e., the creator) or by someone who has been granted permission by the owner. If you are not the owner of the folder or have not been granted permission by the owner, all checkboxes will be gray. Therefore, you will not be able to make any changes until the owner grants you permission.

* Access the *Properties* dialog box.
* Select the ***Security***tab.  
  The top portion of the dialog box lists the users and/or groups that have access to the file or folder.
* Click **Edit**
* In the *Group or user name* section, select the user(s) you wish to set permissions for
* In the *Permissions* section, use the checkboxes to select the appropriate permission level
* Click **Apply**
* Click **Okay**The new permissions are added to the file or folder.
* Advanced Folder Level Permissions

When you set permissions, you specify what users are allowed to do within that folder, such as save and delete files or create a new folder. You are not limited to choosing one of the standard permissions settings (*Full Control, Modify, Read & Execute, List Folder Contents, Read*, or *Write*). Instead of choosing one of these settings, you may set your own unique permissions based on what you would like users to be able to do. For an understanding of how options can be combined, refer to Permission Types: An Overview.

Remember, folder permissions can only be changed by the owner of the folder (i.e., the creator) or by someone who has been granted permission by the owner. If you are not the owner of the folder or have not been granted permission by the owner, the checkboxes will be grayed out. Therefore, you will not be able to make any changes until the owner grants you permission.

* Access the *Properties* dialog box
* Select the ***Security*** tab
* Near the bottom right of the *Properties* dialog box, click **Advanced**The *Advanced Security Settings* dialog box appears.
* (Optional) If you do not want the new folder to have the same permissions as the "parent" (original) folder and wish to set unique permissions for the new folder, click the **Change Permission** button near the bottom. This will bring up a similar window.
  1. Uncheck the ***Include inheritable permissions from this object's parent*** checkbox  
     A *Windows Security* warning dialog box will appear.
  2. Click **Remove** if you want someone removed from permission all together  
     *NOTE: Read the instructions carefully and choose the action you wish to have taken for permissions.*
* Click the **Change Permissions** button
* Select the appropriate user  
  OR  
  Click **Add** and enter the name of the user or group that will have access to the folder.
* Click **Edit**...  
  The *Permissions Entry* dialog box appears.
* In the *Permissions* section, use the checkboxes to set the appropriate permissions  
  *NOTE: If you are not the owner of the folder or have not been granted permission by the owner, all checkboxes will be gray. Therefore you will not be able to make any changes until the owner grants you permission to do so.*
* From the *Apply to:* pull-down list, select what level you wish to apply these permissions to
* Click **OK**
* In the *Advanced Security Setting* dialog box, click **OK**
* Click **OK** from the duplicate *Advanced Security Settings*
* In the *Properties* dialog box, click **OK**The new folder permissions are added for your specified user(s).

6. What is the use of netstat command as well as two switches?

It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement

7. How to find out the information regarding domain name..?

For information about the domain name, including the registrar name, conduct a **search of the public Registration Data Directory Service at https://lookup.icann.org/**. The registrar's name will be included in the result. A list of registrars and links to their websites is on the ICANN -accredited registrar list.

8. What is the use of an advanced scanner?

Advanced IP Scanner is **fast and free software for network scanning**. It will allow you to quickly detect all network computers and obtain access to them. With a single click, you can turn a remote PC on and off, connect to it via Radmin, and much more.

9. How to create the HTTPS website?

**Step 1**

Purchase an SSL certificate. There are a number of companies that offer SSL certificates, including [Verisign.com](http://verisign.com/), [GoDaddy.com](http://godaddy.com/) and [InstantSSL.com](http://instantssl.com/).

**Step 2**

Generate a certificate signing request (CSR) from your web server. Typically, the easiest way is to contact your web server support desk and ask them to do it for you. Each type of web server is different. Most allow you to generate a CSR with their user interface, but it can be a complicated process.

**Step 3**

Submit your CSR to the company you purchased your SSL certificate from. Most SSL companies have a form you can copy and paste the CSR into, but you can always paste it into a text document and email it to them.

**Step 4**

Install your approved SSL certificate on your web server. Once your SSL company verifies your CSR and assigns it to your SSL certificate, they will issue an approved SSL server certificate that must be installed on your web server in order to activate your site security. Again, the easiest way to accomplish this is to contact your web server help desk and ask them to do it for you. Once your SSL certificate is installed you will be able to access your site via HTTPS and your data transfer will be securely encrypted.

10. What is the function of baseline security analysis?

Overview. The Microsoft Baseline Security Analyzer (MBSA) is a **software tool that helps determine the security of your Windows computer based on Microsoft's security recommendations**.

11. How many types of hackers and objectives of hackers as well as phases?

There are 10 types

**1) White Hat Hackers**

White hat hackers are types of hackers who’re professionals with expertise in cybersecurity. They are authorized or certified to hack the systems. These White Hat Hackers work for governments or organizations by getting into the system. They hack the system from the loopholes in the cybersecurity of the organization. This hacking is done to test the level of cybersecurity in their organization. By doing so, they identify the weak points and fix them to avoid attacks from external sources. White hat hackers work as per the rules and regulations set by the government. White hat hackers are also known as ethical hackers.

**Motives & Aims:** The goals of these types of hackers are helping businesses and an appetite for detecting gaps in networks’ security. They aim to protect and assist companies in the ongoing battle against cyber threats. A White Hat hacker is any individual who will help protect the company from raising cyber crimes. They help enterprises create defences, detect vulnerabilities, and solve them before other cybercriminals can find them.

**2) Black Hat Hackers**

Black hat hackers are also knowledgeable computer experts but with the wrong intention. They attack other systems to get access to systems where they do not have authorized entry. On gaining entry they might steal the data or destroy the system. The hacking practices used by these types of hackers depend on the individual’s hacking capacity and knowledge. As the intentions of the hacker make the hacker a criminal. The malicious action intent of the individual cannot be gauged either can the extent of the breach while hacking

**Motives & Aims:** To hack into organizations’ networks and steal bank data, funds or sensitive information. Normally, they use the stolen resources to profit themselves, sell them on the black market or harass their target company.

**3) Gray Hat Hackers**

The intention behind the hacking is considered while categorizing the hacker. The Gray hat hacker falls in between the black hat hackers and white hat hackers. They are not certified, hackers. These types of hackers work with either good or bad intentions. The hacking might be for their gain. The intention behind hacking decides the type of hacker. If the intention is for personal gain then the hacker is considered to be a gray hat hacker.

**Motives & Aims:** The difference is, they don’t want to rob people nor want to help people in particular. Rather, they enjoy experimenting with systems to find loopholes, crack defenses, and generally find a fun hacking experience.

**4) Script Kiddies**

It is a known fact that half knowledge is always dangerous. The Script Kiddies are amateurs types of hackers in the field of hacking. They try to hack the system with scripts from other fellow hackers. They try to hack the systems, networks, or websites. The intention behind the hacking is just to get attention from their peers. Script Kiddies are juveniles who do not have complete knowledge of the hacking process.

**Motives & Aims:** One standard Kiddie Script attack is a DoS (Denial of Service) or DDoS attack (Distributed Denial of Service). This simply means that an IP address is flooded with too many excessive traffic that it collapses. Consider several Black Friday shopping websites, for instance. It creates confusion and prevents someone else uses the service.

**5) Green Hat Hackers**

Green hat hackers are types of hackers who’re learning the ropes of hacking. They are slightly different from the Script Kiddies due to their intention. The intent is to strive and learn to become full-fledged hackers. They are looking for opportunities to learn from experienced hackers.

**6) Blue Hat Hackers**

Blue Hat Hackers are types of hackers who’re similar to Script Kiddies. The intent to learn is missing. They use hacking as a weapon to gain popularity among their fellow beings. They use hacking to settle scores with their adversaries. Blue Hat Hackers are dangerous due to the intent behind the hacking rather than their knowledge.

**7) Red Hat Hackers**

Red Hat Hackers are synonymous with Eagle-Eyed Hackers. They are the types of hackers who’re similar to white hackers. The red hat hackers intend to stop the attack of black hat hackers. The difference between red hat hackers and white hat hackers is in the process of hacking through intention remains the same. Red hat hackers are quite ruthless while dealing with black hat hackers or counteracting with malware. The red hat hackers continue to attack and may end up having to replace the entire system set up.

Above are 7 types of hackers broadly referred to in the cybersecurity world.

The three types of hackers listed below work in different capacities.

**8) State/Nation Sponsored Hackers**

Government appoints hackers to gain information about other countries. These types of hackers are known as State/Nation sponsored hackers. They use their knowledge to gain confidential information from other countries to be well prepared for any upcoming danger to their country. The sensitive information aids to be on top of every situation but also to avoid upcoming danger. They report only to their governments.

**9) Hacktivist**

These types of hackers intend to hack government websites. They pose themselves as activists, so known as a hacktivist. Hacktivist can be an individual or a bunch of nameless hackers whose intent is to gain access to government websites and networks. The data gained from government files accessed are used for personal political or social gain.

**10) Malicious insider or Whistleblower**

These types of hackers include individuals working in an organization who can expose confidential information. The intent behind the exposure might be a personal grudge with the organization or the individual might have come across the illegal activities within the organization. The reason for expose defines the intent behind the exposure. These individuals are known as whistleblowers. .

12. What is the use of NS lookup?

nslookup is an abbreviation of name server lookup and **allows you to query your DNS service**. The tool is typically used to obtain a domain name via your command line interface (CLI), receive IP address mapping details, and lookup DNS records. This information is retrieved from the DNS cache of your chosen DNS server.

13. What is the Function of wire shark and perform the practical?

Wireshark is a **packet sniffer and analysis** tool. It captures network traffic on the local network and stores that data for offline analysis.

14. What is the Mac Address Scanning and Practical?

MAC Address Scan is **a convenient and practical access to the LAN MAC address computer software**.

15. What is The Function of IP Configure and perform the thru switch?

The IP Configuration window configures **the Internet Protocol parameters, allowing the device to receive and send IP packets**. In its factory default configuration, the switch operates as a multiport learning bridge with network connectivity provided by the ports on the switch.

16. Explain the task manager?

A task manager is **a system monitor program used to provide information about the processes and applications running on a computer**, as well as the general status of the computer. Some implementations can also be used to terminate processes and applications, as well as change the processes' scheduling priority.

17. What is the Function of Microsoft Network Monitor?

Microsoft Network Monitor is a deprecated packet analyzer. It **enables capturing, viewing, and analyzing network data and deciphering network protocols**. It can be used to troubleshoot network problems and applications on the network.

18. How to Access the registry in a remote location?

1. Go to **Start >** **Run >** type services.msc
2. Right-click on **Remote Registry** and select **Properties.**
3. Set startup type to **Automatic.**
4. Open the **Run** window again and type regedit.  
   ***NOTE****: Back up the Registry first by going to* ***File > Export*** *and save the registry file.*
5. Configure the following permissions on the registry key below:  
   HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
   * Set Administrators to **Full Control.**
   * Set Local Service to **Read.**
6. Restart **Remote Registry Service** to apply the new settings.

19. How to Block cmd?

To disable Command Prompt with the Windows 10 Registry, use these steps:

* Open **Start**.
* Search for **regedit** and click the top result to open the **Registry Editor**.
* Browse the following path:  
  HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Windows  
  **Quick tip:** On Windows 10, you can now copy and paste the path in the Registry's address bar to quickly jump to the key destination.
* Right-click the **Windows** (folder) key, select the **New** submenu and choose the **Key** option.
* Source: Windows Central
* Name the key **System** and press **Enter**.
* Right-click the **System** (folder) key, select the **New** submenu and choose the **DWORD (32-bit) Value** option.
* Source: Windows Central
* Name the key **DisableCMD** and press **Enter**.
* Double-click the newly created DWORD and set the value from **0** to **2** to disable Command Prompt while allowing batch files to run on the device.
* Source: Windows Central
* (Optional) Double-click the newly created DWORD and set the value from **0** to **1** to disable Command Prompt while preventing batch files from running on Windows 10.
* Click the **OK** button.
* Restart your computer.

20. How to block network Connection?

1. Open Control Panel.
2. In [Windows 10](https://www.lifewire.com/windows-10-2626217), [Windows 8](https://www.lifewire.com/windows-8-2626235), [Windows 7](https://www.lifewire.com/windows-7-2626265), and [Windows Vista](https://www.lifewire.com/windows-vista-2626311), select **Network & Internet**. Alternatively, you can right-click the internet icon in the taskbar (next to the clock) and select **Open Network & Internet settings**.  
   In [Windows XP](https://www.lifewire.com/windows-xp-2626354), change to **Category** view, select **Network and Internet Connections** > **Network Connections**, then skip to Step 4.  
   If your Control Panel doesn't look like the screenshot below, instead having a bunch of icons, try looking for Network and Sharing Center; if you find it you can skip right to Step 4.
3. Select **Network and Sharing Center**.
4. Select **Change adapter settings**. In Windows Vista, choose **Manage network connections**.
5. In the **Network Connections** screen, right-click or tap-and-hold the connection you want to disable, then select **Disable**. The icon for the connection turns grey to show that it's disabled.  
   If **Disable** doesn't appear in the menu, the connection is disabled.
6. If prompted, confirm the action, or enter an admin password if you're not logged in as an administrator.
7. The internet connection is disabled.