CIS Center for Internet Security®

CIS Controls®

Exploited Protocols:

Remote Desktop Protocol (RDP)

NOVEMBER 2020

Contents

Acknowledgments

The Center for Internet Security® (CIS®) would like to thank the many security experts who volunteer their time and talent to support the CIS Controls® and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Editors
Valecia Stocchetti, CIS

Contributors
Ginger E. Anderson, CIS
Jennifer Jarose, CIS
Phyllis Lee, CIS
Robin Regnier, CIS
Phil White, CIS
Thomas Sager, CIS

Introduction

The CIS Critical Security Controls® (CIS Controls®) are a prioritized set of actions which collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of Information Technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors, including retail, manufacturing, healthcare, education, government, defense, and others. While the CIS Controls address the general practices that most organizations should take to secure their systems, some operational environments may present unique requirements not addressed by the CIS Controls.

We are at a point in cybersecurity where offense must inform defense in order to help protect against the most prolific cyber threats to our environments. Telecommuting has always presented challenges, balancing security with usability. Open-source reports indicate that Remote Desktop Protocol (RDP) usage jumped an estimated 41% when COVID-19 struck. While many organizations have been prepared for a global pandemic (maybe without even being aware that they were), others were left scrambling to stand up remote environments for employees to utilize, many of which were likely left unsecure and vulnerable to attackers. COVID-19 didn't necessarily shift the threat landscape, because remote environments have always been a desired target for attackers to conduct a cyber-attack. However, COVID-19 did increase the attack surface, with more people than ever telecommuting. In a world where organizations already have multiple threats to defend against, a shift such as this one can be somewhat overwhelming for organizations to safeguard against those threats.

Purpose

The Microsoft® Remote Desktop Services (RDS), formerly known as Terminal Services, is a service that is used to remotely connect to another system through a network connection. RDP is the protocol that is used for RDS, running over port 3389 (Transmission Control Protocol (TCP)/User Datagram Protocol (UDP)) by default. While RDP is generally associated with Windows-based operating systems, there are similar implementations for other operating systems, such as macOS®, Linux®, and Android™. Microsoft formally defines RDP as:

> "The Microsoft Remote Desktop Protocol (RDP) provides remote display and input capabilities over network connections for Windows-based applications running on a server. RDP is designed to support different types of network topologies and multiple LAN protocols. RDP is based on, and an extension of, the ITU T.120 family of protocols. RDP is a multiple-channel capable protocol that allows for separate virtual channels for carrying device communication and presentation data from the server, as well as encrypted client mouse and keyboard data. RDP provides an extensible base and supports up to 64,000 separate channels for data transmission and provisions for multipoint transmission." (Microsoft, 2018)

Open-source intelligence tells us that over 3.5 million internet-connected devices have RDP open publicly. To clarify, that does not mean that all of those devices are actively being exploited; however, it does mean that the surface area is vast for attackers. The Multi-State Information Security & Analysis Center® (MS-ISAC®) data tells us that RDP remains one of the top attacked protocols.

While many types of attacks utilize RDP, a solution as drastic as "turn off RDP completely" may not be a viable or realistic option for an organization. Some applications and systems require the use of RDP in order to carry out day-to-day business functions. Additionally, there are multiple points in a network where RDP can be enabled/disabled. It is not a one-size-fits-all approach.

A more appropriate approach to this problem is for organizations that use RDP to use it securely. Just like a piece of wood can be used to build a home, it can also be used as a dangerous weapon, and the same concept applies here. While RDP in and of itself is not dangerous, leaving it unsecured can make it an appealing target for attackers.

The purpose of this guide is to provide an overview of what RDP is, the attacks associated with this protocol, and how an organization can best protect itself against an RDP-based attack.

Attacks Using RDP

Cybercriminals will almost always choose the path of least resistance when it comes to exploiting a system or network. Attackers no longer have to go through great lengths to exploit a system using highly customized tools and techniques. They can simply use what is right in front of them to access a system. This becomes a frightening concept in the world of security, because the lines of attacker behavior versus normal user behavior become blurred, making it more difficult to detect an intrusion.

Not surprisingly, ransomware, a type of malware that blocks access to a device until ransom is paid, continues to be a top threat for many different sectors around the globe. Historically, a typical ransomware infection did not involve an attacker exploiting a system or network hands-on. Rather, the ransomware was executed automatically through an exploit kit, such as the well-known Angler exploit kit in 2015. However, in more recent years, ransomware has shifted the threat landscape significantly and now includes what Microsoft is calling "human-operated ransomware."

According to the Microsoft Digital Defense Report, September 2020: "Human-operated ransomware is sometimes referred to as 'big game ransomware,' a term that implies cybercriminals select specific networks for their value proposition and then hunt for entry vectors. This approach has been the exception, not the rule, in most major ransomware attacks in the past year. Cybercriminals perform massive wide-ranging sweeps of the internet, searching for vulnerable entry points. Or they enter networks via 'commodity' Trojans and then 'bank' this access for a time and purpose that's advantageous to them." (Microsoft Digital Defense Report, 2020).

Among these vulnerable entry points, RDP is included as a top attack vector. There are multiple ways that an RDP-based ransomware attack can occur, including phishing. This is where an attacker tricks a user into entering their credentials into a fake webpage and later uses them to log into the system legitimately. Then, using brute-force, an attacker will try numerous different passwords until the right one is entered, granting them access. Once inside the network, an attacker can move laterally to expand their reach. Some techniques that are common include elevating administrative privileges, installing backdoors, setting up fake user accounts, and deploying ransomware to other systems on the network.

Even worse, within the past year, RDP-based ransomware attacks have been combined with banking Trojans, such as Emotet, TrickBot, QakBot, IcedID, and Dridex. These Trojans are particularly troublesome because they can harvest additional credentials, spread throughout the network automatically, scrape email addresses to send out phishing emails, and download additional malware. Organizations that become infected with ransomware face a difficult decision. They have to decide whether to pay the ransom to get back their data, decline to pay and recover from backups, or decrypt the data with an online decryptor. However, decryption is very rare these days, since the more prevalent types of ransomware do not have decryptors available online.

Paying the ransom is not recommended, as it encourages criminals to continue their operations. However, it is ultimately a business decision whether or not an organization decides to pay as no one wants to be the next headline in the news. That being said, implementing the necessary mitigations and best practices to protect against an RDP-based attack will pay off in the long run.

Benefits of RDP

RDP has many business benefits:

- End-users are able to connect to organizational systems from home, or while they are away, using a graphical user interface (GUI).
- For organizations on a limited budget, purchasing expensive software to set up a remote environment may not always be feasible. Therefore, utilizing RDP may be the only available option.
- The ability to harness the remote system's full processing power, which is especially beneficial when running very resource-intensive applications. This, in turn, also reduces the need to purchase additional hardware to support those who may work both in the office and at home.
- Another benefit that may not always be visible is an increase in productivity for employees. In the current world where many organizations shifted quickly to a remote environment, it is critical to keep employees happy. If multiple barriers are put in an employee's way, it will only tempt them more to break security policies in order to "get the job done." Without providing a secure remote protocol to access organizational assets, employees may send sensitive data to their personal assets, or upload them to unsecure cloud providers. While maintaining a secure environment should always be a top priority, a balance between usability and security should be kept in mind when making decisions that will impact an organization's workforce.

How to Use This Guide

This guide is intended to assist organizations that would like to start implementing the use of RDP, or want to know how to best secure RDP if it's already in use. CIS has combined mitigations and best practices from CIS Controls and CIS Benchmarks™ to deliver a singular document that organizations can use to secure RDP with confidence, as well as understand the types of RDP-based attacks that an organization might face.

Each section provides:

- A high-level overview of the direct mitigation for securing RDP, followed by the applicable CIS Controls and/or CIS Benchmarks™
- CIS Controls include, and are ordered by, their respective mapping to the NIST Cybersecurity Framework (NIST CSF)

In addition, supportive controls for protecting against RDP-based attacks are included in Appendix A of this guide. A listing of all applicable CIS Controls and Benchmarks, can be found in Appendices B and C of this guide.

Direct Mitigations for Securing RDP

The controversy with RDP has been long debated in the security community. While RDP does have known vulnerabilities, it can be argued that so do many other applications. As with any piece of technology, securing it is key. As stated previously, it is not a one-size-fits-all approach, as RDP can be a risk on many different levels within a network (network, host, application level, etc.).

Overall, there are seven direct mitigations for securing RDP, many of which are of low or no cost to an organization, and are discussed on the next few pages:

- Place RDP-enabled systems behind a Remote Desktop Gateway (RDG) or virtual private network (VPN)
- Update and patch software that uses RDP
- Limit access to RDP by internet protocol (IP) and port
- Use complex, unique passwords for RDP-enabled accounts
- Implement a session lockout for RDP-enabled accounts
- Disconnect idle RDP sessions
- Secure Remote Desktop Session Host

Below, we will discuss mitigations that can be put in place to lock down RDP directly, why it is important from an attack perspective, and how the mitigation can be implemented.

Place RDP-Enabled Systems Behind a Remote Desktop Gateway (RDG) or Virtual Private Network (VPN)

Why is this important?

When deploying or configuring endpoints and servers internal to an organization's network, it is recommended that they are not exposed directly to the internet with RDP enabled. As stated previously, many attackers are continuously scanning for systems that are internet-connected and have ports that can be exploited. RDP is one of those ports that is highly desirable to attackers. That is not to say that RDP cannot be opened at all on an endpoint or server—it just needs to be done thoughtfully.

How can this be implemented?

If RDP is needed, it is recommended that the systems are put behind a virtual private network (VPN) or that a Remote Desktop Gateway (RDG) server is set up. The organization's budget may determine whether to purchase a VPN or utilize the Microsoft native RDG service. This added layer of security will do a few things. First, it will prevent attackers from easily identifying which systems on the organization's internal network are accessible via RDP from the internet. Second, it will force a user to authenticate to the corporate network (through the VPN or RDG) before authenticating to the internal system via RDP. This will help determine which users are authorized to connect via RDP. RDG also allows IT to control which resources users can access and the type of authentication they are required to use, such as multi-factor authentication (MFA). If it is not possible to implement a VPN or RDG and the organization must have a system exposed directly to the internet with RDP, then it is recommended that other mitigating controls, such as complex passwords and multi-factor authentication for RDP user accounts, are put in place to reduce the risk of a successful attack. In addition to the above, running automated vulnerability scanning tools and performing regular automated port scans will help to detect any systems that may have RDP exposed directly to the internet and, as a result, may be vulnerable to an RDP-based attack.

Related CIS Sub-Controls:

- 9.1 — Associate Active Ports, Services, and Protocols to Asset Inventory (Identify)
- 3.3 — Protect Dedicated Assessment Accounts (Protect)
- 5.1 — Establish Secure Configurations (Protect)
- 9.2 — Ensure Only Approved Ports, Protocols, and Services Are Running (Protect)
- 3.1 — Run Automated Vulnerability Scanning Tools (Detect)
- 3.2 — Perform Authenticated Vulnerability Scanning (Detect)
- 9.3 — Perform Regular Automated Port Scans (Detect)

Update and Patch Software That Uses RDP

Why is this important?

Attackers thrive when they find systems that are unpatched or vulnerable to exploits, making it critical that organizations keep operating systems, and any software that uses RDP, patched and up-to-date. An unpatched, out-of-date system is more likely to have vulnerabilities known to attackers, either previously discovered or reverse-engineered from the patch that addressed it.

How can this be implemented?

Deploying automated operating systems and software patch management tools will help ensure that an organization has the latest security updates that are provided by the software vendor. Our CIS Microsoft Windows® 10 Benchmarks have several configurations that can be applied to enable automatic updates, as shown below. Additionally, patching not only needs to be timely, but also conducted on a regular basis. For servers and other business-critical systems, patches should be tested in a testing environment to be sure they will not negatively affect the organization's production environment, when possible.

Related CIS Sub-Controls:

- 3.4 — Deploy Automated Operating System Patch Management Tools (Protect)
- 3.5 — Deploy Automated Software Patch Management Tools (Protect)

Related CIS Microsoft Windows 10 Enterprise Release 2004 Benchmark v1.9.0:

- 18.9.102.2 — (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'
- 18.9.102.3 — (L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'
- 18.9.102.4 — (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'
- 18.9.102.5 — (L1) Ensure 'Remove access to 'Pause updates' feature' is set to 'Enabled'

Limit Access to RDP by IP and Port

Why is this important?

RDP-based attacks generally begin at the perimeter and can continue once an attacker gains access to a network, allowing them to move laterally to other endpoints. Limiting access to RDP by Internet Protocol (IP) address and port helps control that traffic flowing outside of and within a network.

How can this be implemented?

This can be achieved by implementing a network-based and host-based firewall. By doing so, an organization has the ability to block unwanted traffic and connections. Both a network-based and host-based firewall should be utilized and properly configured. For network-based firewalls, block any inbound RDP connections from accessing an internal system directly. For internal systems requiring RDP access, utilize a VPN or RDG, as mentioned previously. While the default port for RDP is 3389, note that port numbers can be changed from the default, so it is best to double-check which port RDP is running on before implementing these rules.

For host-based firewalls, deny inbound RDP connections from external systems that are not authorized to access the system, only allowing authorized systems access. For systems that need to be accessed via RDP, block inbound connections and manually "allowlist" any IP addresses that need access. This will ensure only authorized users have the ability to RDP into a system. For any systems that do not need RDP enabled, block inbound connections to these systems completely.

Related CIS Sub-Controls:

- 9.1 — Associate Active Ports, Services, and Protocols to Asset Inventory (Identify)
- 9.2 — Ensure Only Approved Ports, Protocols, and Services Are Running (Protect)
- 9.4 — Apply Host-Based Firewalls or Port-Filtering (Protect)
- 12.3 — Deny Communications with Known Malicious IP Addresses (Protect)
- 12.4 — Deny Communication Over Unauthorized Ports (Protect)
- 12.7 — Deploy Network-Based Intrusion Prevention Systems (Protect)
- 14.2 — Enable Firewall Filtering Between VLANs (Protect)
- 9.3 — Perform Regular Automated Port Scans (Detect)

Use Complex, Unique Passwords for RDP-Enabled Accounts

Why is this important?

According to the 2020 Verizon Data Breach Investigations Report (DBIR), phishing (social engineering) and malicious password dumpers are among the top four actions in small and large organization breaches. While weak and common passwords are not exclusive to RDP-based attacks, they do remain one of the top attack vectors, as stated previously.

Passwords are ubiquitous and will likely remain so for a long time. Attackers don't necessarily need a password to get into a system via RDP. They can always rely on other methods, such as software vulnerabilities, to get in. However, having a weak password is equivalent to having a front door lock that is broken, not installed properly, or just leaving the door completely unlocked. A homeowner would likely not do any of those things with their front door if they are trying to prevent a burglar from getting in, so an organization should do the same for its systems and data.

How can this be implemented?

When user accounts with RDP enabled are set up, it is important to ensure that password complexity is enforced, especially for administrative user accounts (as these will have additional privileges beyond RDP). Recently, CIS published a Password Policy Guide using guidance from both NIST and Microsoft to provide best practices when it comes to authentication. Among those recommendations is the use of a 14-character password if no multi-factor authentication (MFA) is enforced, or an 8-character password for accounts with MFA enabled. Techniques, such as using passphrases, are also encouraged, as they tend to be longer, harder to crack, and easier for employees to remember. The most important thing to keep in mind is that password complexity is a balance. The more complex a password policy becomes, the more risk the organization runs of its employees using workarounds.

More best practices can be found within the CIS Password Policy Guide, here.

Related CIS Sub-Controls:

- 4.2 — Change Default Passwords (Protect)
- 4.4 — Use Unique Passwords (Protect)

Related CIS Microsoft Windows 10 Enterprise Release 2004 Benchmark v1.9.0:

- 18.9.62.3.9.1 — (L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'
- 18.9.62.2.2 — (L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'
- 1.1.1 — (L1) Ensure 'Enforce password history' is set to '24 or more password(s)'
- 1.1.2 — (L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'
- 1.1.3 — (L1) Ensure 'Minimum password age' is set to '1 or more day(s)'
- 1.1.4 — (L1) Ensure 'Minimum password length' is set to '14 or more character(s)'
- 1.1.5 — (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'
- 1.1.6 — (L1) Ensure 'Relax minimum password length limits' is set to 'Enabled'
- 1.1.7 — (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'

Implement a Session Lockout for RDP-Enabled Accounts

Why is this important?

Attackers will often utilize brute-force attack techniques against accounts with RDP enabled in an attempt to compromise a network. This can consist of either a prolonged attack, where the attempts occur over a longer period of time, or a distributed attack, where the attempts occur in short bursts with a high number of logins. Limiting failed login attempts by implementing an account lockout will help reduce the risk of a successful brute-force attack.

How can this be implemented?

Based on the CIS Password Policy Guide, it is recommended to implement a temporary account lockout (15 minutes or more) after five consecutive failed attempts or time doubling throttling (in minutes) between each retry (0, 1, 2, 4, 8, etc.). After 12 retries, a permanent account lockout where it is required to contact IT to reset the account should be implemented. In addition to setting policies around failed logon attempts, logging and alerting of this activity should also be enabled.

Related CIS Microsoft Windows 10 Enterprise Release 2004 Benchmark v1.9.0:

- 1.2.1 — (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)'
- 1.2.2 — (L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'
- 1.2.3 — (L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'
- 2.3.7.3 — (BL) Ensure 'Interactive logon: Machine account lockout threshold' is set to '10 or fewer invalid logon attempts, but not 0'

Disconnect Idle RDP Sessions

Why is this important?

RDP session hijacking, where an attacker is able to resume an active session, is one way that a system or network can be compromised. It allows the attacker to take control of an RDP session that has not been disconnected. This is why, with RDP sessions, the recommended action is to disconnect the session after a period of inactivity. This will not only protect any active, but idle, sessions from being hijacked by an attacker, but will also open up the available sessions for other authorized users to authenticate to.

How can this be implemented?

For endpoints using Remote Desktop Services (RDS), the CIS Microsoft Windows 10 Benchmarks have a series of recommendations, which are shown below.

Related CIS Microsoft Windows 10 Enterprise Release 2004 Benchmark v1.9.0:

- 18.9.62.3.10.1 — (L2) Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less'
- 18.9.62.3.10.2 — (L2) Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute'

- 2.3.7.4 — (L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'
- 2.3.7.9 — (L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher

Secure Remote Desktop Session Host

Why is this important?

Securing an organization's RDP connections are an absolute must for those using RDP. There are many concerns with credentials, most notably their storage and transmission, which is why all credentials should be encrypted in transit and at rest when connecting via RDP.

How can this be implemented?

To implement encryption during transmittal, the CIS Microsoft Windows 10 Benchmarks recommends a few best practices:

- Set "Require use of specific security layer for RDP connections" to "Enabled: Secure Socket Layer (SSL)." By setting this policy, it requires the use of a specific security layer to secure communications between clients and remote desktop session host servers during an RDP connection.
- Set "Require user authentication for remote connections by using Network Level Authentication (NLA)" to "Enabled." Enabling NLA adds another layer of security by requiring a user to authenticate to the RD Session Host server before establishing a remote desktop session. In order to enable NLA, the client must be running Remote Desktop Connection version 6.0 or later. The client must also be using an operating system that supports the Credential Security Support Provider (CredSSP) protocol. The RD Session Host server must also be running Windows Server 2008 or higher. While having NLA enabled won't protect an organization against all RDP-based attacks, it will help reduce the exploitation of a vulnerability, as it only allows authenticated users access to the network.
- Set "Set client connection encryption level" to "Enabled: High Level."
- Ensure "Require secure RPC communication" is set to "Enabled."
- Ensure "Encryption Oracle Remediation" is set to "Enabled: Force Updated Clients."

Combined, these settings will set a user's remote desktop session to the highest security level possible, and mitigate the risk of an attacker obtaining credentials and authenticating via RDP.

Related CIS Sub-Controls:

- 12.12 — Manage All Devices Remotely Logging Into Internal Network (Protect)
- 16.2 — Configure Centralized Point of Authentication (Protect)
- 16.4 — Encrypt or Hash All Authentication Credentials (Protect)
- 16.5 — Encrypt Transmittal of Username and Authentication Credentials (Protect)

Related CIS Microsoft Windows 10 Enterprise Release 2004 Benchmark v1.9.0:

- 18.9.62.3.9.2 — (L1) Ensure 'Require secure RPC communication' is set to 'Enabled'
- 18.9.62.3.9.3 — (L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL'
- 18.9.62.3.9.4 — (L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled'
- 18.9.62.3.9.5 — (L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'
- 18.8.4.1 — (L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients'

Conclusion

Overall, these RDP-based attacks can flourish not because their targets lack the most expensive software or application, but rather because they lack basic cyber hygiene. Many of the mitigations and best practices in this guide can be implemented with no or low cost to the organization. By implementing these CIS Controls and CIS Benchmarks, organizations can effectively strengthen their cybersecurity posture to help protect against RDP-based attacks.

CIS Controls®

APPENDIX A:

Supportive Controls for Protecting Against RDP-Based Attacks

There are also a number of best practices that do not protect RDP directly, but rather act as supportive controls for protecting against an RDP-based attack. Separate RDP-enabled systems via network segmentation can be broken into six main instructions:

- Implement multi—factor authentication (MFA) with VPN/RDG
- Delete or disable dormant accounts, and restrict administrative privileges that have RDP enabled
- Keep inventory and control of hardware and software assets that use RDP
- Follow the Least Privilege model when granting RDP permissions
- Protect data from an RDP—based attack
- Log and monitor for RDP—related events

More information on these seven supportive controls are explained below.

Separate RDP-Enabled Systems via Network Segmentation

Why is this important?

For RDP-based attacks, having network segmentation implemented is critical, especially if there are sensitive systems within the network that do not have a need for RDP to be open. From an attacker perspective, network segmentation can make it more difficult to cause widespread damage and also can protect those sensitive systems, if configured properly. A flat network, or one without segmentation, means that all systems are on one network. While a flat network costs significantly less to implement, it can also be a breeding ground for attackers and malware, as they are able to do more damage in a shorter amount of time.

How can this be implemented?

Network segmentation, which is defined as separating a network into two or more subnetworks (called subnets), should be segmented based on the sensitivity of the asset. Sensitive systems should reside on a network separate from, for example, a group of systems that have RDP enabled. If kept on the same subnet as systems with RDP enabled, it can increase the risk of an attacker carrying out an RDP-based attack, allowing them to easily pivot to, and compromise, those sensitive systems.

Furthermore, networks that are segmented can still be a point of weakness if not configured properly. Locking down access between subnets is key to avoiding a widespread RDP-based attack across subnets. If administrative access is needed between subnets, use a technology, such as a jump server, to carry out these administrative tasks. A jump server is a system that is used to access and manage systems that have multiple subnets.

If network segmentation is not possible, then mitigating controls, including secure authorization and authentication methods, should be in place to reduce the risk of an RDP-based attack. Additionally, a Zero Trust model for networks can be followed. Zero Trust is a relatively newer concept in security in which a user, regardless of whether they are located internal or external to the network, is considered a threat. As a result, every device or user requesting access to a system is required to authenticate. This is where the Least Privilege model, discussed later, should be implemented.

Related CIS Sub-Controls:

- 12.1 — Maintain an Inventory of Network Boundaries (Identify)
- 14.1 — Segment the Network Based on Sensitivity (Protect)
- 12.2 — Scan for Unauthorized Connections Across Trusted Network Boundaries (Detect)

Implement Multi-Factor Authentication with VPN/RDG

Why is this important?

Passwords are just one facet of security. MFA, a method in which two or more credentials are provided for authenticating, should be implemented to protect against an RDP-based attack. There are multiple factors that can be requested when authorizing access to a system or application, such as something you know (e.g., password), something you have (e.g., smartcard, token), or something you are (e.g., fingerprint, retina). Two-factor authentication, another common term, is simply using two methods for authenticating. However, more than two methods can be implemented, depending on the sensitivity of the system or application. Additionally, just because there are multiple layers of authentication does not mean that one of the methods, such as a password, can be weakened.

How can this be implemented?

Implementation of MFA will depend on the configuration of an organization's network. For organizations using a VPN or RDG, implementing MFA at the gateway will reduce the risk of an attacker gaining unauthorized access to systems within the network. For organizations that do not use a VPN or RDG and have internet-connected systems that require RDP to be enabled, MFA should be implemented, where possible. For any organization or system that cannot implement MFA, mitigating controls, such as complex passwords and session lockouts/timeouts, must be implemented.

Related CIS Sub-Controls:

- 4.5 — Use Multi—Factor Authentication for All Administrative Access (Protect)
- 11.5 — Manage Network Devices Using Multi—Factor Authentication and Encrypted Sessions (Protect)
- 12.11 — Require All Remote Logins to Use Multi—Factor Authentication (Protect)
- 16.3 — Require Multi—Factor Authentication (Protect)

Delete or Disable Dormant Accounts, and Restrict Administrative Privileges That Have RDP Enabled

Why is this important?

Deleting or disabling dormant user accounts, especially those with RDP enabled, should be a part of an organization's processes and procedures. In order to know which accounts are dormant, an organization needs to maintain an inventory of those accounts, including identifying which accounts have administrative privileges or are able to use RDP. Dormant accounts are a prime target for attackers, especially accounts that have permission to RDP into the network or have administrative level access. When controls such as account management fall to the wayside, it allows attackers to not only compromise the system or network, but also go undetected for long periods of time if there is no monitoring enabled for these accounts.

How can this be implemented?

An organization should use dedicated accounts and workstations for administrative purposes and tasks, especially when using RDP to connect. By separating these from normal user accounts, the organization lowers the risk of an attacker compromising a highly privileged administrator account. Additionally, by separating these accounts and workstations, an organization can easily tune logging to monitor and detect anomalous behavior more quickly. Logging will be discussed in detail later in this guide.

Disabling or deleting dormant accounts, as well as establishing a process for revoking access for employees or contractors/third-parties who may no longer need access or have left the organization, will help mitigate the risk of attackers compromising rogue accounts. Ensuring that accounts have an expiration date, and that they are monitored and enforced, will also help with account management. For example, if a third-party vendor is on a contract for three months, and an organization knows the completion date of their contract, they could set the account expiration to the date the contract ends so that they are unable to use that account once their work is complete. If the contract is extended, they can always re-enable the account and set a new expiration date.

Related CIS Sub-Controls:

- 16.1 — Maintain an Inventory of Authentication Systems (Identify)
- 16.6 — Maintain an Inventory of Accounts (Identify)
- 4.3 — Ensure the Use of Dedicated Administrative Accounts (Protect)
- 4.6 — Use Dedicated Workstations for All Administrative Tasks (Protect)
- 16.7 — Establish Process for Revoking Access (Protect)
- 16.10 — Ensure All Accounts Have an Expiration Date (Protect)
- 4.1 — Maintain Inventory of Administrative Accounts (Detect)
- 16.8 — Disable Any Unassociated Accounts (Respond)
- 16.9 — Disable Dormant Accounts (Respond)

Related CIS Microsoft Windows 10 Enterprise Release 2004 Benchmark v1.9.0:

- 2.3.1.1 — (L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled'
- 2.3.1.2 — (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'

- 2.3.1.3 — (L1) Ensure 'Accounts: Guest account status' is set to 'Disabled'
- 2.3.1.4 — (L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'
- 2.3.1.5 — (L1) Configure 'Accounts: Rename administrator account'
- 2.3.1.6 — (L1) Configure 'Accounts: Rename guest account'

Keep Inventory and Control of Hardware and Software Assets that Use RDP

Why is this important?

The first step of the incident response life cycle—preparation—is arguably the most important. Organizations must take the necessary steps to prepare against a cyber-attack before it actually happens. In this case, to defend against an RDP-based attack, an organization needs to know which hardware and software assets they are responsible for in order to protect them. By not doing so, an organization runs the risk of an attacker compromising a system—or worse, a network making the incident response process difficult to determine which system or application is responsible for the attack. This level of difficulty increases as the number of systems on a network increases, especially if the organization has no inventory system.

How can this be implemented?

When locking down RDP, taking an inventory of which systems have RDP enabled is critical. CIS Control 1, Inventory and Control of Hardware Assets, and CIS Control 2, Inventory and Control of Software Assets, are applicable in this case. While they are important Controls, they can also be the most challenging to implement. For organizations that do not have a formal inventory system for hardware and software, CIS offers a spreadsheet that can be easily used for tracking these assets that can be found here.

Related CIS Sub-Controls:

- 1.1 — Utilize an Active Discovery Tool (Identify)
- 1.2 — Use a Passive Asset Discovery Tool (Identify)
- 1.4 — Maintain Detailed Asset Inventory (Identify)
- 1.5 — Maintain Asset Inventory Information (Identify)
- 2.1 — Maintain Inventory of Authorized Software (Identify)
- 2.2 — Ensure Software is Supported by Vendor (Identify)
- 2.3 — Utilize Software Inventory Tools (Identify)
- 2.4 — Track Software Inventory Information (Identify)
- 2.5 — Integrate Software and Hardware Asset Inventories (Identify)
- 1.7 — Deploy Port Level Access Control (Protect)
- 1.8 — Utilize Client Certificates to Authenticate Hardware Assets (Protect)
- 1.6 — Address Unauthorized Assets (Respond)
- 2.6 — Address Unapproved Software (Respond)

Follow the Least Privilege Model When Granting RDP Permissions

Why is this important?

Following a Least Privilege model ensures that only those who have a need are granted access. It is far easier to grant a user the minimum amount of privileges needed for their job, and assign when needed, than to over-provision. When granting permissions for users to log in via RDP, an organization will want to ensure that only users who need the access are granted access. All other users should be removed to avoid an attacker compromising a user account through RDP.

How can this be implemented?

As with many of these best practices, taking an inventory of accounts to see which users have the capability to log on via RDP is a good place to start. Once the list is established, review it to assess who still needs access and who does not. An organization should ideally incorporate these practices during an employee's onboarding, and then audit as needed.

Often, IT professionals use RDP to access a system remotely for administration. Organizations may also open up RDP on an endpoint device to allow authorized users to access their desktop remotely. The CIS Microsoft Windows Benchmark recommends the following:

- Set "Access this computer from the network" to "Administrators, Remote Desktop Users" and set "Allow log on locally" to "Administrators, Users." These two recommendations will need to be enabled when allowing incoming RDP connections.
- Set "Allow log on through Remote Desktop Services" to "Administrators, Remote Desktop Users."
- For any local or guest accounts on the system (including service accounts), enable the "Deny log on through Remote Desktop Services" rule. These types of accounts are appealing to an attacker, especially if the accounts are granted a wide array of permissions. Additionally, if these accounts are not monitored, it can give the attacker the ability to remain undetected on the network, potentially for an extended period of time.

If an organization is deploying any of these settings, it is recommended that they use a centralized management and configuration tool, such as Group Policy, to grant access. To add another layer of security to RDP, an organization can choose to only allow RDP connections from certain approved IP addresses, via "allowlisting."

Related CIS Microsoft Windows 10 Enterprise Release 2004 Benchmark v1.9.0:

- 2.2.2 — (L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'
- 2.2.5 — (L1) Ensure 'Allow log on locally' is set to 'Administrators, Users'
- 2.2.6 — (L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'
- 2.2.20 — (L1) Ensure 'Deny log on through Remote Desktop Services' is set to include 'Guests, Local account'
- 18.8.36.1 — (L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'
- 18.8.36.2 — (L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'

Protect Data From an RDP-Based Attack

Why is this important?

Data is often an organization's most coveted asset and should be protected as such. In general, data protection can be achieved by following the CIA triad: *confidentiality, integrity,* and *availability*. Especially as organizations shift towards cloud computing, it is imperative to know where the data is stored and how to best protect it in order to limit the risk of data compromise or exfiltration. RDP-based attacks involving the deployment of ransomware have increased rapidly over the past few years, which is why organizations should take the necessary action to protect their data. Without data protection mitigations in place, it becomes very easy for an attacker to exfiltrate or delete data, disrupt operations, and even potentially cause physical damage, should they gain access to the system or network.

How can this be implemented?

When it comes to data protection, there are multiple safeguards that can be put into place. The following are best practices that CIS recommends:

- Separate the data by sensitivity. Keep an organization's critical assets and data away from less sensitive data, such as information on public—facing systems.
- Back up data on a regular basis. For more sensitive systems in an organization, take full backups through a process such as imaging, which will allow for quick recovery should an incident occur.
- Test backups on a regular basis to confirm that they are working properly.
- Protect backups through physical security and encryption, when they are being stored or moving across a network, to avoid backups from becoming modified or destroyed in the event of a ransomware attack. This includes any remote backups and cloud services.
- Have at least one offline destination for backups, meaning that they are not accessible through a network connection, to help avoid backups from becoming corrupted. If backups are not in an offline location, an organization runs the risk of the backups being encrypted or, even worse, completely deleted by an attacker (manually) or by the ransomware (automatically).
- Know what sensitive information is being stored, processed, or transmitted and where it is being stored. Any sensitive information that no longer needs to be accessed should be removed. If a system needs to be accessed periodically, then that system should be taken off the network or virtualized and powered off until needed.
- Protect data by encrypting sensitive data in transit and at rest, when following the confidentiality feature of the CIA triad.

More specific best practices can be offered by the CIS Microsoft Windows 10 Benchmark:

- Set "Do not allow drive redirection" to "Enabled." This will prevent users from sharing local drives on their client computers to Remote Desktop Servers that they access. Without having this setting enabled, it leaves shared local drives vulnerable for an attacker to exploit the data. This also goes for clipboard data that can be stored within an RDP session, as an attacker may be able to scrape data that is copied. The setting "Do not allow clipboard redirection" should be set to "Enabled" to help reduce the risk of this data being compromised.
- Set "Do not delete temp folders upon exit" to "Disabled." This will avoid having Remote Desktop Services (RDS) retain a user's temporary folders after logging off.

Related CIS Sub-Controls:

- 13.1 — Maintain an Inventory of Sensitive Information (Identify)
- 10.1 — Ensure Regular Automated Backups (Protect)
- 10.2 — Perform Complete System Backups (Protect)
- 10.3 — Test Data on Backup Media (Protect)
- 10.4 — Protect Backups (Protect)
- 10.5 — Ensure All Backups Have at Least One Offline Backup Destination (Protect)
- 13.2 — Remove Sensitive Data or Systems Not Regularly Accessed by Organization (Protect)
- 14.4 — Encrypt All Sensitive Information in Transit (Protect)
- 14.6 — Protect Information Through Access Control Lists (Protect)
- 14.7 — Enforce Access Control to Data Through Automated Tools (Protect)
- 14.8 — Encrypt Sensitive Information at Rest (Protect)
- 14.5 — Utilize an Active Discovery Tool to Identify Sensitive Data (Detect)

CIS Microsoft Windows 10 Enterprise Release 1909 Benchmark v1.8.1:

- 18.9.62.3.3.2 — (L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'
- 18.9.62.3.11.1 — (L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'
- 2.3.7.2 — (L1) Ensure 'Interactive logon: Don't display last signed—in' is set to 'Enabled'
- 18.8.4.2 — (L1) Ensure 'Remote host allows delegation of non—exportable credentials' is set to 'Enabled'
- 18.8.28.1 — (L1) Ensure 'Block user from showing account details on sign—in' is set to 'Enabled'

Log and Monitor for RDP-Related Events

Why is this important?

While preventive controls are certainly helpful in mitigating attacks, detective controls are also needed when all else fails. Logging and monitoring RDP events will help identify when an attacker is attempting to exploit or has exploited a system/network. Having logs enabled and configured correctly is the first step in identifying potential adverse events.

How can this be implemented?

CIS offers the following best practices for logging and monitoring:

- Enable local audit logging on all systems and networking devices. Additionally, enable detailed logging to help assist with investigating a potential event or incident.
- Keep logs in one location for ease of analysis and review, using a central log management solution.
- Review logs to identify any abnormal activity or anomalies that may be occurring. To help with the analysis of logs, some organizations decide to deploy analytical tools, such as a Security Information and Event Management (SIEM), to correlate and analyze the logs. Organizations will want to ensure that their SIEM is tuned on a regular basis to decrease the number of false positives and to better identify actionable events.
- Determine who (or what application) will be responsible for monitoring these logs. While most of the analysis can be automated, if an adverse event is identified, a process must be in place on how to address that event. Some organizations may choose to have a team of in—house analysts to review events and filter out what needs to be investigated. Others may choose to outsource their monitoring to a Managed Security Services Provider (MSSP), where a dedicated team is responsible for managing their security—related services.
- Determine which logs need to be stored, and set a retention period based on organizational need. Note that state and federal regulations may apply in some cases. Also ensure that adequate storage is allocated for the logs.

When it comes to RDP-specific logs, there are various Event IDs and Logon Types to pay close attention to. Below are just a few suggestions that can help an organization identify a successful or failed RDP logon.

- To identify an initial network connection via RDP, first review the Microsoft—Windows—Terminal—Services—RemoteConnectionManager/Operational log, specifically Event ID 1149, which will indicate when a user has launched an RDP client and made a network connection to the target system. Note that this does not necessarily mean that an attacker has exploited a system yet.
- To identify if a user has successfully authenticated via RDP, review the Microsoft Windows Security Event Log. Review Event ID 4624, with Logon Types 3 (Network), 7 (Unlock), or 10 (Remote Interactive). Note that Type 3 is present when NLA is enabled, Type 7 can occur if a previous RDP session was not logged out, and Type 10 can occur right after a Type 3 logon to the network.
- Another log that can help identify successful RDP logons is the Microsoft—Windows—TerminalServices—RDPClient/Operational Event Log, specifically Event IDs 1024, 1025, 1026, 1028, 1029, and 1105.
- Successful and failed logons should be reviewed. Knowing when an RDP logon failed, especially multiple times, can raise a potential red flag for the security team to investigate. Failed logons will be stored in the Microsoft Windows Security Event Log, with an Event ID 4625 and Logon Type of either 3 (if NLA is enabled) or 10 (if NLA is not enabled).
- The Microsoft—Windows—TerminalServices—LocalSessionManager Event Log is also helpful in analyzing RDP connections. Specifically pay attention to Event IDs 21 and 24 recorded in this log.

- The RemoteDesktopServices—RDPCoreTS/Operational Event Log can reveal additional information about the logon, including the user's IP address (Event IDs 131 and 140), which can be used during incident response to identify the scope of the compromise.

In general, for logs that are being monitored, pay close attention to the hours of the day and week that failed logons are occurring via RDP, as well as the timing of those attempts. For example, if multiple users are trying to RDP into the system at midnight and have multiple failed attempts, configure the monitoring device to flag on that behavior, specific to the security policy that an organization has set forth.

Related CIS Sub-Controls:

- 4.8 — Log and Alert on Changes to Administrative Group Membership (Detect)
- 4.9 — Log and Alert on Unsuccessful Administrative Account Login (Detect)
- 6.2 — Activate Audit Logging (Detect)
- 6.3 — Enable Detailed Logging (Detect)
- 6.4 — Ensure Adequate Storage for Logs (Detect)
- 6.5 — Central Log Management (Detect)
- 6.6 — Deploy SIEM or Log Analytic Tools (Detect)
- 6.7 — Regularly Review Logs (Detect)
- 6.8 — Regularly Tune SIEM (Detect)
- 12.6 — Deploy Network—Based IDS Sensors (Detect)
- 12.8 — Deploy NetFlow Collection on Networking Boundary Devices (Detect)
- 12.10 — Decrypt Network Traffic at Proxy (Detect)
- 13.3 — Monitor and Block Unauthorized Network Traffic (Detect)
- 13.5 — Monitor and Detect Any Unauthorized Use of Encryption (Detect)
- 14.9 — Enforce Detail Logging for Access or Changes to Sensitive Data (Detect)
- 16.12 — Monitor Attempts to Access Deactivated Accounts (Detect)
- 16.13 — Alert on Account Login Behavior Deviation (Detect)

Related CIS Microsoft Windows 10 Enterprise Release 2004 Benchmark v1.9.0:

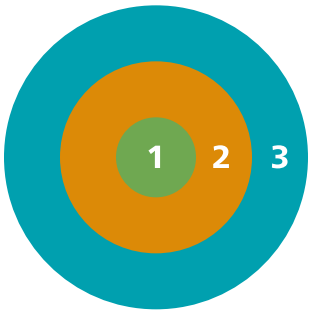
- 17.5.5 — (L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'

CIS Controls®

APPENDIX B:
CIS Controls

Implementation Groups

As a part of our most recent version of the CIS Controls, v7.1, we created Implementation Groups (IGs) to provide granularity and some explicit structure to the different realities faced by organizations of varied sizes.



Definitions	1	2	3
Implementation Group 1 CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. IG1 represents basic cyber hygiene for all organizations including those in IG2 and IG3.	●		
Implementation Group 2 CIS Sub-Controls (safeguards) focused on helping organizations handling more sensitive assets and data. IG2 safeguards should also be followed by organizations in IG3.	●	●	
Implementation Group 3 CIS Sub-Controls (safeguards) are necessary for organizations that handle critical assets and data. IG3 encompasses safeguards in IG1 and IG2.	●	●	●

IG1

A Group 1 organization is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these organizations is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data they are trying to protect is low and principally involves employee and financial information. However, there may be some small to medium-sized organizations that are responsible for protecting sensitive data and, therefore, will fall into a higher group. Sub-Controls selected for Group 1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Sub-Controls will also typically be designed to work in conjunction with small or home office Commercial-off-the-Shelf (COTS) hardware and software.

IG2

A Group 2 organization employs individuals responsible for managing and protecting IT infrastructure. These organizations support multiple departments with different risk profiles based on job function and mission. Small organizational units may have regular compliance burdens. Group 2 organizations often store and process sensitive client or company information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Sub-Controls selected for Group 2 help security teams cope with increased operational complexity. Some Sub-Controls will depend on enterprise-grade technology and specialized expertise to properly install and configure.

IG3

A Group 3 organization employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). Group 3 systems and data contain sensitive information or functions that are subject to regulatory and compliance oversight. A Group 3 organization must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Sub-Controls selected for Group 3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

If you would like to know more about the Implementation Groups and how they pertain to organizations of all sizes, there are many resources that explore the Implementation Groups and the CIS Controls in general at our website at https://www.cisecurity.org/controls/cis-controls-list/.

CIS Controls: RDP-Related Recommendations

Below is a list of CIS Sub-Controls associated with securing RDP.

CIS Control	CIS Sub-Control	Asset Type	Security Function	CIS Control Title	IG1	IG2	IG3	RDP-Related Recommendation	Direct Mitigation or Supportive Control?
9	9.1	Devices	Identify	Associate Active Ports, Services, and Protocols to Asset Inventory		●	●	Place RDP-Enabled Systems Behind a Remote Desktop Gateway (RDG) or Virtual Private Network (VPN)	Direct Mitigation
3	3.3	Users	Protect	Protect Dedicated Assessment Accounts		●	●	Place RDP-Enabled Systems Behind a Remote Desktop Gateway (RDG) or Virtual Private Network (VPN)	Direct Mitigation
5	5.1	Applications	Protect	Establish Secure Configurations	●	●	●	Place RDP-Enabled Systems Behind a Remote Desktop Gateway (RDG) or Virtual Private Network (VPN)	Direct Mitigation
9	9.2	Devices	Protect	Ensure Only Approved Ports, Protocols, and Services Are Running		●	●	Place RDP-Enabled Systems Behind a Remote Desktop Gateway (RDG) or Virtual Private Network (VPN)	Direct Mitigation
3	3.1	Applications	Detect	Run Automated Vulnerability Scanning Tools		●	●	Place RDP-Enabled Systems Behind a Remote Desktop Gateway (RDG) or Virtual Private Network (VPN)	Direct Mitigation
3	3.2	Applications	Detect	Perform Authenticated Vulnerability Scanning		●	●	Place RDP-Enabled Systems Behind a Remote Desktop Gateway (RDG) or Virtual Private Network (VPN)	Direct Mitigation
9	9.3	Devices	Detect	Perform Regular Automated Port Scans		●	●	Place RDP-Enabled Systems Behind a Remote Desktop Gateway (RDG) or Virtual Private Network (VPN)	Direct Mitigation

CIS Control	CIS Sub-Control	Asset Type	Security Function	CIS Control Title	IG1	IG2	IG3	RDP-Related Recommendation	Direct Mitigation or Supportive Control?
3	3.4	Applications	Protect	Deploy Automated Operating System Patch Management Tools	●	●	●	Update and Patch Software That Uses RDP	Direct Mitigation
3	3.5	Applications	Protect	Deploy Automated Software Patch Management Tools	●	●	●	Update and Patch Software That Uses RDP	Direct Mitigation
9	9.1	Devices	Identify	Associate Active Ports, Services, and Protocols to Asset Inventory		●	●	Limit Access to RDP by IP and Port	Direct Mitigation
9	9.2	Devices	Protect	Ensure Only Approved Ports, Protocols, and Services Are Running		●	●	Limit Access to RDP by IP and Port	Direct Mitigation
9	9.4	Devices	Protect	Apply Host-Based Firewalls or Port-Filtering	●	●	●	Limit Access to RDP by IP and Port	Direct Mitigation
12	12.3	Network	Protect	Deny Communications with Known Malicious IP Addresses		●	●	Limit Access to RDP by IP and Port	Direct Mitigation
12	12.4	Network	Protect	Deny Communication Over Unauthorized Ports	●	●	●	Limit Access to RDP by IP and Port	Direct Mitigation
12	12.7	Network	Protect	Deploy Network-Based Intrusion Prevention Systems			●	Limit Access to RDP by IP and Port	Direct Mitigation
14	14.2	Network	Protect	Enable Firewall Filtering Between VLANs		●	●	Limit Access to RDP by IP and Port	Direct Mitigation
9	9.3	Devices	Detect	Perform Regular Automated Port Scans		●	●	Limit Access to RDP by IP and Port	Direct Mitigation
4	4.2	Users	Protect	Change Default Passwords	●	●	●	Use Complex, Unique Passwords for RDP-Enabled Accounts	Direct Mitigation
4	4.4	Users	Protect	Use Unique Passwords		●	●	Use Complex, Unique Passwords for RDP-Enabled Accounts	Direct Mitigation
12	12.12	Devices	Protect	Manage All Devices Remotely Logging into Internal Network			●	Secure Remote Desktop Session Host	Direct Mitigation
16	16.2	Users	Protect	Configure Centralized Point of Authentication		●	●	Secure Remote Desktop Session Host	Direct Mitigation
16	16.4	Users	Protect	Encrypt or Hash all Authentication Credentials		●	●	Secure Remote Desktop Session Host	Direct Mitigation
16	16.5	Users	Protect	Encrypt Transmittal of Username and Authentication Credentials		●	●	Secure Remote Desktop Session Host	Direct Mitigation
12	12.1	Network	Identify	Maintain an Inventory of Network Boundaries	●	●	●	Separate RDP-Enabled Systems via Network Segmentation	Supportive Control
14	14.1	Network	Protect	Segment the Network Based on Sensitivity		●	●	Separate RDP-Enabled Systems via Network Segmentation	Supportive Control
12	12.2	Network	Detect	Scan for Unauthorized Connections Across Trusted Network Boundaries		●	●	Separate RDP-Enabled Systems via Network Segmentation	Supportive Control
4	4.5	Users	Protect	Use Multi-Factor Authentication for All Administrative Access		●	●	Implement Multi-Factor Authentication With VPN/RDG	Supportive Control

CIS Control	CIS Sub-Control	Asset Type	Security Function	CIS Control Title	IG1	IG2	IG3	RDP-Related Recommendation	Direct Mitigation or Supportive Control?
11	11.5	Network	Protect	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions		●	●	Implement Multi-Factor Authentication With VPN/RDG	Supportive Control
12	12.11	Users	Protect	Require All Remote Login to Use Multi-Factor Authentication		●	●	Implement Multi-Factor Authentication With VPN/RDG	Supportive Control
16	16.3	Users	Protect	Require Multi-Factor Authentication		●	●	Implement Multi-Factor Authentication With VPN/RDG	Supportive Control
16	16.1	Users	Identify	Maintain an Inventory of Authentication Systems		●	●	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control
16	16.6	Users	Identify	Maintain an Inventory of Accounts		●	●	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control
4	4.3	Users	Protect	Ensure the Use of Dedicated Administrative Accounts	●	●	●	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control
4	4.6	Users	Protect	Use Dedicated Workstations for All Administrative Tasks		●	●	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control
16	16.7	Users	Protect	Establish Process for Revoking Access		●	●	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control
16	16.10	Users	Protect	Ensure All Accounts Have an Expiration Date		●	●	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control
4	4.1	Users	Detect	Maintain Inventory of Administrative Accounts		●	●	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control
16	16.8	Users	Respond	Disable Any Unassociated Accounts	●	●	●	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control
16	16.9	Users	Respond	Disable Dormant Accounts	●	●	●	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control
1	1.1	Devices	Identify	Utilize an Active Discovery Tool		●	●	Keep Inventory and Control of Hardware and Software Assets That Use RDP	Supportive Control
1	1.2	Devices	Identify	Use a Passive Asset Discovery Tool			●	Keep Inventory and Control of Hardware and Software Assets That Use RDP	Supportive Control
1	1.4	Devices	Identify	Maintain Detailed Asset Inventory	●	●	●	Keep Inventory and Control of Hardware and Software Assets That Use RDP	Supportive Control
1	1.5	Devices	Identify	Maintain Asset Inventory Information		●	●	Keep Inventory and Control of Hardware and Software Assets That Use RDP	Supportive Control
2	2.1	Applications	Identify	Maintain Inventory of Authorized Software	●	●	●	Keep Inventory and Control of Hardware and Software Assets That Use RDP	Supportive Control
2	2.2	Applications	Identify	Ensure Software is Supported by Vendor	●	●	●	Keep Inventory and Control of Hardware and Software Assets That Use RDP	Supportive Control
2	2.3	Applications	Identify	Utilize Software Inventory Tools		●	●	Keep Inventory and Control of Hardware and Software Assets That Use RDP	Supportive Control

CIS Control	CIS Sub-Control	Asset Type	Security Function	CIS Control Title	IG1	IG2	IG3	RDP-Related Recommendation	Direct Mitigation or Supportive Control?
2	2.4	Applications	Identify	Track Software Inventory Information		●	●	Keep Inventory and Control of Hardware and Software Assets That Use RDP	Supportive Control
2	2.5	Applications	Identify	Integrate Software and Hardware Asset Inventories			●	Keep Inventory and Control of Hardware and Software Assets That Use RDP	Supportive Control
1	1.7	Devices	Protect	Deploy Port Level Access Control		●	●	Keep Inventory and Control of Hardware and Software Assets That Use RDP	Supportive Control
1	1.8	Devices	Protect	Utilize Client Certificates to Authenticate Hardware Assets			●	Keep Inventory and Control of Hardware and Software Assets That Use RDP	Supportive Control
1	1.6	Devices	Respond	Address Unauthorized Assets	●	●	●	Keep Inventory and Control of Hardware and Software Assets That Use RDP	Supportive Control
2	2.6	Applications	Respond	Address Unapproved Software	●	●	●	Keep Inventory and Control of Hardware and Software Assets That Use RDP	Supportive Control
13	13.1	Data	Identify	Maintain an Inventory of Sensitive Information	●	●	●	Protect Data From an RDP-Based Attack	Supportive Control
10	10.1	Data	Protect	Ensure Regular Automated Backups	●	●	●	Protect Data From an RDP-Based Attack	Supportive Control
10	10.2	Data	Protect	Perform Complete System Backups	●	●	●	Protect Data From an RDP-Based Attack	Supportive Control
10	10.3	Data	Protect	Test Data on Backup Media		●	●	Protect Data From an RDP-Based Attack	Supportive Control
10	10.4	Data	Protect	Protect Backups	●	●	●	Protect Data From an RDP-Based Attack	Supportive Control
10	10.5	Data	Protect	Ensure All Backups Have at Least One Offline Backup Destination	●	●	●	Protect Data From an RDP-Based Attack	Supportive Control
13	13.2	Data	Protect	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	●	●	●	Protect Data From an RDP-Based Attack	Supportive Control
14	14.4	Data	Protect	Encrypt All Sensitive Information in Transit		●	●	Protect Data From an RDP-Based Attack	Supportive Control
14	14.6	Data	Protect	Protect Information Through Access Control Lists	●	●	●	Protect Data From an RDP-Based Attack	Supportive Control
14	14.7	Data	Protect	Enforce Access Control to Data Through Automated Tools			●	Protect Data From an RDP-Based Attack	Supportive Control
14	14.8	Data	Protect	Encrypt Sensitive Information at Rest			●	Protect Data From an RDP-Based Attack	Supportive Control
14	14.5	Data	Detect	Utilize an Active Discovery Tool to Identify Sensitive Data			●	Protect Data From an RDP-Based Attack	Supportive Control
4	4.8	Users	Detect	Log and Alert on Changes to Administrative Group Membership		●	●	Log and Monitor for RDP-Related Events	Supportive Control
4	4.9	Users	Detect	Log and Alert on Unsuccessful Administrative Account Login		●	●	Log and Monitor for RDP-Related Events	Supportive Control

CIS Control	CIS Sub-Control	Asset Type	Security Function	CIS Control Title	IG1	IG2	IG3	RDP-Related Recommendation	Direct Mitigation or Supportive Control?
6	6.2	Network	Detect	Activate Audit Logging	●	●	●	Log and Monitor for RDP-Related Events	Supportive Control
6	6.3	Network	Detect	Enable Detailed Logging		●	●	Log and Monitor for RDP-Related Events	Supportive Control
6	6.4	Network	Detect	Ensure Adequate Storage for Logs		●	●	Log and Monitor for RDP-Related Events	Supportive Control
6	6.5	Network	Detect	Central Log Management		●	●	Log and Monitor for RDP-Related Events	Supportive Control
6	6.6	Network	Detect	Deploy SIEM or Log Analytic Tools		●	●	Log and Monitor for RDP-Related Events	Supportive Control
6	6.7	Network	Detect	Regularly Review Logs		●	●	Log and Monitor for RDP-Related Events	Supportive Control
6	6.8	Network	Detect	Regularly Tune SIEM			●	Log and Monitor for RDP-Related Events	Supportive Control
12	12.6	Network	Detect	Deploy Network-Based IDS Sensors		●	●	Log and Monitor for RDP-Related Events	Supportive Control
12	12.8	Network	Detect	Deploy NetFlow Collection on Networking Boundary Devices		●	●	Log and Monitor for RDP-Related Events	Supportive Control
12	12.10	Network	Detect	Decrypt Network Traffic at Proxy			●	Log and Monitor for RDP-Related Events	Supportive Control
13	13.3	Data	Detect	Monitor and Block Unauthorized Network Traffic			●	Log and Monitor for RDP-Related Events	Supportive Control
13	13.5	Data	Detect	Monitor and Detect Any Unauthorized Use of Encryption			●	Log and Monitor for RDP-Related Events	Supportive Control
14	14.9	Data	Detect	Enforce Detail Logging for Access or Changes to Sensitive Data			●	Log and Monitor for RDP-Related Events	Supportive Control
16	16.12	Users	Detect	Monitor Attempts to Access Deactivated Accounts		●	●	Log and Monitor for RDP-Related Events	Supportive Control
16	16.13	Users	Detect	Alert on Account Login Behavior Deviation			●	Log and Monitor for RDP-Related Events	Supportive Control

CIS Controls®

APPENDIX C:
CIS Benchmarks

CIS Benchmarks: RDP-Related Recommendations

Below is a list of CIS Benchmarks associated with securing RDP. Note that each Benchmark is designated with L1 (Level 1) or L2 (Level 2). The Level 1 profile is considered a base recommendation that can be implemented fairly promptly and is designed to not have an extensive performance impact. The intent of the Level 1 profile Benchmark is to lower the attack surface of an organization while keeping machines usable and not hindering business functionality.

The Level 2 profile is considered to be "defense-in-depth" and is intended for environments where security is paramount. The recommendations associated with the Level 2 profile can have an adverse effect on an organization if not implemented appropriately or without due care.

CIS Benchmark Section #	CIS Benchmark Recommendation #	CIS Benchmark Title and Description	RDP-Related Recommendation	Direct Mitigation or Supportive Control
18.9.102	18.9.102.2	**(L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'** This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them. After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work: **2** Notify for download and auto install _(Notify before downloading any updates)_ **3** Auto download and notify for install _(Download the updates automatically and notify when they are ready to be installed.) (Default setting)_ **4** Auto download and schedule the install _(Automatically download updates and install them on the schedule specified below.))_ **5** Allow local admin to choose setting _(Leave decision on above choices up to the local Administrators (Not Recommended))_ The recommended state for this setting is: 'Enabled' **Note #1:** The sub-setting '_Configure automatic updating:_' has 4 possible values – all of them are valid depending on specific organizational needs, however if feasible we suggest using a value of '4 – Auto download and schedule the install.' This suggestion is not a scored requirement. **Note #2:** Organizations that utilize a 3rd-party solution for patching may choose to exempt themselves from this recommendation, and instead configure it to 'Disabled' so that the native Windows Update mechanism does not interfere with the 3rd-party patching process.	Update and Patch Software that Uses RDP	Direct Mitigation
18.9.102	18.9.102.3	**(L1) Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 – Every day'** This policy setting specifies when computers in your environment will receive security updates from Windows Update or WSUS. The recommended state for this setting is: '0 – Every day' **Note:** This setting is only applicable if '4 – Auto download and schedule the install' is selected in Rule 18.9.102.2. It will have no impact if any other option is selected.	Update and Patch Software that Uses RDP	Direct Mitigation

CIS Benchmark Section #	CIS Benchmark Recommendation #	CIS Benchmark Title and Description	RDP-Related Recommendation	Direct Mitigation or Supportive Control
18.9.102	18.9.102.4	**(L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'** This policy setting specifies that Automatic Updates will wait for computers to be restarted by the users who are logged on to them to complete a scheduled installation. The recommended state for this setting is: 'Disabled.' **Note:** This setting applies only when you configure Automatic Updates to perform scheduled update installations. If you configure the Configure Automatic Updates setting to Disabled, this setting has no effect.	Update and Patch Software that Uses RDP	Direct Mitigation
18.9.102	18.9.102.5	**(L1) Ensure 'Remove access to 'Pause updates' feature' is set to 'Enabled'** This policy removes access to 'Pause updates' feature. The recommended state for this setting is: 'Enabled.'	Update and Patch Software that Uses RDP	Direct Mitigation
18.9.62.3.9	18.9.62.3.9.1	**(L1) Ensure 'Always prompt for password upon connection' is set to 'Enabled'** This policy setting specifies whether Remote Desktop Services always prompts the client computer for a password upon connection. You can use this policy setting to enforce a password prompt for users who log on to Remote Desktop Services, even if they already provided the password in the Remote Desktop Connection client. The recommended state for this setting is: 'Enabled.'	Use Complex, Unique Passwords for RDP-Enabled Accounts	Direct Mitigation
18.9.62.2	18.9.62.2.2	**(L1) Ensure 'Do not allow passwords to be saved' is set to 'Enabled'** This policy setting helps prevent Remote Desktop clients from saving passwords on a computer. The recommended state for this setting is: 'Enabled.' **Note:** If this policy setting was previously configured as Disabled or Not configured, any previously saved passwords will be deleted the first time a Remote Desktop client disconnects from any server.	Use Complex, Unique Passwords for RDP-Enabled Accounts	Direct Mitigation
1.1	1.1.1	**(L1) Ensure 'Enforce password history' is set to '24 or more password(s)'** This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password. The recommended state for this setting is: '24 or more password(s).' **Note:** Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.	Use Complex, Unique Passwords for RDP-Enabled Accounts	Direct Mitigation

CIS Benchmark Section #	CIS Benchmark Recommendation #	CIS Benchmark Title and Description	RDP-Related Recommendation	Direct Mitigation or Supportive Control
1.1	1.1.2	**(L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'** This policy setting defines how long a user can use their password before it expires. Values for this policy setting range from 0 to 999 days. If you set the value to 0, the password will never expire. Because attackers can crack passwords, the more frequently you change the password the less opportunity an attacker has to use a cracked password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support due to users having to change their password or forgetting which password is current. The recommended state for this setting is '60 or fewer days, but not 0.' **Note:** Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.	Use Complex, Unique Passwords for RDP-Enabled Accounts	Direct Mitigation
1.1	1.1.3	**(L1) Ensure 'Minimum password age' is set to '1 or more day(s)'** This policy setting determines the number of days that you must use a password before you can change it. The range of values for this policy setting is between 1 and 999 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this setting is 0 days. The recommended state for this setting is: '1 or more day(s)).' **Note:** Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.	Use Complex, Unique Passwords for RDP-Enabled Accounts	Direct Mitigation
1.1	1.1.4	**(L1) Ensure 'Minimum password length' is set to '14 or more character(s)'** This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "passphrase" is a better term than "password." In Microsoft Windows 2000 and newer, passphrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid passphrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length. In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements. The recommended state for this setting is: '14 or more character(s).' **Note #1:** In Windows Server 2016 and older versions of Windows Server, the GUI of the Local Security Policy (LSP), Local Group Policy Editor (LGPE) and Group Policy Management Editor (GPME) would not let you set this value higher than 14 characters. However, starting with Windows Server 2019, Microsoft changed the GUI to allow up to a 20 character minimum password length. **Note #2:** Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.	Use Complex, Unique Passwords for RDP-Enabled Accounts	Direct Mitigation

CIS Benchmark Section #	CIS Benchmark Recommendation #	CIS Benchmark Title and Description	RDP-Related Recommendation	Direct Mitigation or Supportive Control
1.1	1.1.5	**(L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled'** This policy setting checks all new passwords to ensure that they meet basic requirements for strong passwords. When this policy is enabled, passwords must meet the following minimum requirements: – Not contain the user's account name or parts of the user's full name that exceed two consecutive characters – Be at least six characters in length – Contain characters from three of the following categories: – English uppercase characters (A through Z) – English lowercase characters (a through z) – Base 10 digits (0 through 9) – Non-alphabetic characters (for example, !, $, #, %) – A catch-all category of any Unicode character that does not fall under the previous four categories. This fifth category can be regionally specific. Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 267 (approximately 8 x 109 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 527 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 268 (or 2 x 1011) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@." Proper use of the password settings can help make it difficult to mount a brute-force attack. The recommended state for this setting is: 'Enabled.' **Note:** Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.	Use Complex, Unique Passwords for RDP-Enabled Accounts	Direct Mitigation
1.1	1.1.6	**(L1) Ensure 'Relax minimum password length limits' is set to 'Enabled'** This policy setting determines whether the minimum password length setting can be increased beyond the legacy limit of 14 characters. For more information please see the following [Microsoft Security Blog](https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-baseline-draft-windows-10-and-windows-server-version/ba-p/1419213). The recommended state for this setting is: 'Enabled.' **Note:** This setting only affects _local_ accounts on the computer. Domain accounts are only affected by settings on the Domain Controllers, because that is where domain accounts are stored.	Use Complex, Unique Passwords for RDP-Enabled Accounts	Direct Mitigation

CIS Benchmark Section #	CIS Benchmark Recommendation #	CIS Benchmark Title and Description	RDP-Related Recommendation	Direct Mitigation or Supportive Control
1.1	1.1.7	**(L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled'** This policy setting determines whether the operating system stores passwords in a way that uses reversible encryption, which provides support for application protocols that require knowledge of the user's password for authentication purposes. Passwords that are stored with reversible encryption are essentially the same as plaintext versions of the passwords. The recommended state for this setting is: 'Disabled.' **Note:** Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.	Use Complex, Unique Passwords for RDP-Enabled Accounts	Direct Mitigation
1.2	1.2.1	**(L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)'** This policy setting determines the length of time that must pass before a locked account is unlocked and a user can try to log on again. The setting does this by specifying the number of minutes a locked out account will remain unavailable. If the value for this policy setting is configured to 0, locked out accounts will remain locked out until an administrator manually unlocks them. Although it might seem like a good idea to configure the value for this policy setting to a high value, such a configuration will likely increase the number of calls that the help desk receives to unlock accounts locked by mistake. Users should be aware of the length of time a lock remains in place, so that they realize they only need to call the help desk if they have an extremely urgent need to regain access to their computer. The recommended state for this setting is: '15 or more minute(s).' **Note:** Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.	Implement a Session Lockout for RDP-Enabled Accounts	Direct Mitigation
1.2	1.2.2	**(L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'** This policy setting determines the number of failed logon attempts before the account is locked. Setting this policy to '0' does not conform to the benchmark as doing so disables the account lockout threshold. The recommended state for this setting is: '10 or fewer invalid logon attempt(s), but not 0.' **Note:** Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.	Implement a Session Lockout for RDP-Enabled Accounts	Direct Mitigation

CIS Benchmark Section #	CIS Benchmark Recommendation #	CIS Benchmark Title and Description	RDP-Related Recommendation	Direct Mitigation or Supportive Control
1.2	1.2.3	**(L1) Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'** This policy setting determines the length of time before the Account lockout threshold resets to zero. The default value for this policy setting is Not Defined. If the Account lockout threshold is defined, this reset time must be less than or equal to the value for the Account lockout duration setting. If you leave this policy setting at its default value or configure the value to an interval that is too long, your environment could be vulnerable to a DoS attack. An attacker could maliciously perform a number of failed logon attempts on all users in the organization, which will lock out their accounts. If no policy were determined to reset the account lockout, it would be a manual task for administrators. Conversely, if a reasonable time value is configured for this policy setting, users would be locked out for a set period until all of the accounts are unlocked automatically. The recommended state for this setting is: '15 or more minute(s).' **Note:** Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.	Implement a Session Lockout for RDP-Enabled Accounts	Direct Mitigation
2.3.7	2.3.7.3	**(BL) Ensure 'Interactive logon: Machine account lockout threshold' is set to '10 or fewer invalid logon attempts, but not 0'** This security setting determines the number of failed logon attempts that causes the machine to be locked out. Failed password attempts against workstations or member servers that have been locked using either CTRL+ALT+DELETE or password protected screen savers counts as failed logon attempts. The machine lockout policy is enforced only on those machines that have BitLocker enabled for protecting OS volumes. Please ensure that appropriate recovery password backup policies are enabled. The recommended state for this setting is: '10 or fewer invalid logon attempts, but not 0.' **Note:** A value of '0' does not conform to the benchmark as it disables the machine account lockout threshold. Values from '1' to '3' will be interpreted as '4.'	Implement a Session Lockout for RDP-Enabled Accounts **Note: BL represents BitLocker.	Direct Mitigation
18.9.62.3.10	18.9.62.3.10.1	**(L2) Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less'** This policy setting allows you to specify the maximum amount of time that an active Remote Desktop Services session can be idle (without user input) before it is automatically disconnected. The recommended state for this setting is: 'Enabled: 15 minutes or less.'	Disconnect Idle RDP Sessions	Direct Mitigation
18.9.62.3.10	18.9.62.3.10.2	**(L2) Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute'** This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions. The recommended state for this setting is: 'Enabled: 1 minute.'	Disconnect Idle RDP Sessions	Direct Mitigation
2.3.7	2.3.7.4	**(L1) Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'** Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session. The recommended state for this setting is: '900 or fewer second(s), but not 0.' **Note:** A value of '0' does not conform to the benchmark as it disables the machine inactivity limit.	Disconnect Idle RDP Sessions	Direct Mitigation

CIS Benchmark Section #	CIS Benchmark Recommendation #	CIS Benchmark Title and Description	RDP-Related Recommendation	Direct Mitigation or Supportive Control
2.3.7	2.3.7.9	**(L1) Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher** This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader. The recommended state for this setting is: 'Lock Workstation.' Configuring this setting to 'Force Logoff' or 'Disconnect if a Remote Desktop Services session' also conforms to the benchmark.	Disconnect Idle RDP Sessions	Direct Mitigation
18.9.62.3.9	18.9.62.3.9.2	**(L1) Ensure 'Require secure RPC communication' is set to 'Enabled'** This policy setting allows you to specify whether Remote Desktop Services requires secure Remote Procedure Call (RPC) communication with all clients or allows unsecured communication. You can use this policy setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests. The recommended state for this setting is: 'Enabled.'	Secure Remote Desktop Session Host	Direct Mitigation
18.9.62.3.9	18.9.62.3.9.3	**(L1) Ensure 'Require use of specific security layer for remote (RDP) connections' is set to 'Enabled: SSL'** This policy setting specifies whether to require the use of a specific security layer to secure communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections. The recommended state for this setting is: 'Enabled: SSL.' **Note:** In spite of this setting being labelled _SSL_, it is actually enforcing Transport Layer Security (TLS) version 1.0, not the older (and less secure) SSL protocol.	Secure Remote Desktop Session Host	Direct Mitigation
18.9.62.3.9	18.9.62.3.9.4	**(L1) Ensure 'Require user authentication for remote connections by using Network Level Authentication' is set to 'Enabled'** This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication. The recommended state for this setting is: 'Enabled.'	Secure Remote Desktop Session Host	Direct Mitigation
18.9.62.3.9	18.9.62.3.9.5	**(L1) Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'** This policy setting specifies whether to require the use of a specific encryption level to secure communications between client computers and RD Session Host servers during Remote Desktop Protocol (RDP) connections. This policy only applies when you are using native RDP encryption. However, native RDP encryption (as opposed to SSL encryption) is not recommended. This policy does not apply to SSL encryption. The recommended state for this setting is: 'Enabled: High Level.'	Secure Remote Desktop Session Host	Direct Mitigation
18.8.4	18.8.4.1	**(L1) Ensure 'Encryption Oracle Remediation' is set to 'Enabled: Force Updated Clients'** Some versions of the CredSSP protocol that is used by some applications (such as Remote Desktop Connection) are vulnerable to an encryption oracle attack against the client. This policy controls compatibility with vulnerable clients and servers and allows you to set the level of protection desired for the encryption oracle vulnerability. The recommended state for this setting is: 'Enabled: Force Updated Clients.'	Secure Remote Desktop Session Host	Direct Mitigation
2.3.1	2.3.1.1	**(L1) Ensure 'Accounts: Administrator account status' is set to 'Disabled'** This policy setting enables or disables the Administrator account during normal operation. When a computer is booted into safe mode, the Administrator account is always enabled, regardless of how this setting is configured. Note that this setting will have no impact when applied to the Domain Controllers organizational unit via Group Policy because Domain Controllers have no local account database. It can be configured at the domain level via Group Policy, similar to account lockout and password policy settings. The recommended state for this setting is: 'Disabled.'	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control

CIS Benchmark Section #	CIS Benchmark Recommendation #	CIS Benchmark Title and Description	RDP-Related Recommendation	Direct Mitigation or Supportive Control
2.3.1	2.3.1.2	**(L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'** This policy setting prevents users from adding new Microsoft accounts on this computer. The recommended state for this setting is: 'Users can't add or log on with Microsoft accounts.'	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control
2.3.1	2.3.1.3	**(L1) Ensure 'Accounts: Guest account status' is set to 'Disabled'** This policy setting determines whether the Guest account is enabled or disabled. The Guest account allows unauthenticated network users to gain access to the system. The recommended state for this setting is: 'Disabled.' **Note:** This setting will have no impact when applied to the Domain Controllers organizational unit via Group Policy because Domain Controllers have no local account database. It can be configured at the domain level via Group Policy, similar to account lockout and password policy settings.	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control
2.3.1	2.3.1.4	**(L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'** This policy setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. If you enable this policy setting, local accounts that have blank passwords will not be able to log on to the network from remote client computers. Such accounts will only be able to log on at the keyboard of the computer. The recommended state for this setting is: 'Enabled.'	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control
2.3.1	2.3.1.5	**(L1) Configure 'Accounts: Rename administrator account'** The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this account, and to avoid names that denote administrative or elevated access accounts. Be sure to also change the default description for the local administrator (through the Computer Management console).	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control
2.3.1	2.3.1.6	**(L1) Configure 'Accounts: Rename guest account'** The built-in local guest account is another well-known name to attackers. It is recommended to rename this account to something that does not indicate its purpose. Even if you disable this account, which is recommended, ensure that you rename it for added security.	Delete or Disable Dormant Accounts & Restrict Administrative Privileges That Have RDP Enabled	Supportive Control
2.2	2.2.2	**(L1) Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'** This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)-based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+). The recommended state for this setting is: 'Administrators, Remote Desktop Users.'	Follow the Least Privilege Model When Granting RDP Permissions	Supportive Control
2.2	2.2.5	**(L1) Ensure 'Allow log on locally' is set to 'Administrators, Users'** This policy setting determines which users can interactively log on to computers in your environment. Logons that are initiated by pressing the CTRL+ALT+DEL key sequence on the client computer keyboard require this user right. Users who attempt to log on through Terminal Services / Remote Desktop Services or IIS also require this user right. The recommended state for this setting is: 'Administrators, Users.' **Note:** The 'Guest' account is also assigned this user right by default. Although this account is disabled by default, it's recommended that you configure this setting through Group Policy. However, this user right should generally be restricted to the 'Administrators' and 'Users' groups. Assign this user right to the 'Backup Operators' group if your organization requires that they have this capability.	Follow the Least Privilege Model When Granting RDP Permissions	Supportive Control

CIS Benchmark Section #	CIS Benchmark Recommendation #	CIS Benchmark Title and Description	RDP-Related Recommendation	Direct Mitigation or Supportive Control
2.2	2.2.6	**(L1) Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'** This policy setting determines which users or groups have the right to log on as a Remote Desktop Services client. If your organization uses Remote Assistance as part of its help desk strategy, create a group and assign it this user right through Group Policy. If the help desk in your organization does not use Remote Assistance, assign this user right only to the 'Administrators' group or use the Restricted Groups feature to ensure that no user accounts are part of the 'Remote Desktop Users' group. Restrict this user right to the 'Administrators' group, and possibly the 'Remote Desktop Users' group, to prevent unwanted users from gaining access to computers on your network by means of the Remote Assistance feature. The recommended state for this setting is: 'Administrators, Remote Desktop Users.' **Note #1:** The above list is to be treated as a whitelist, which implies that the above principals need not be present for assessment of this recommendation to pass. **Note #2:** In all versions of Windows prior to Windows 7, **Remote Desktop Services** was known as **Terminal Services**, so you should substitute the older term if comparing against an older OS.	Follow the Least Privilege Model When Granting RDP Permissions	Supportive Control
2.2	2.2.20	**(L1) Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'** This policy setting determines whether users can log on as Remote Desktop clients. After the baseline workstation is joined to a domain environment, there is no need to use local accounts to access the workstation from the network. Domain accounts can access the workstation for administration and end-user processing. This user right supersedes the **Allow log on through Remote Desktop Services** user right if an account is subject to both policies. The recommended state for this setting is to include: 'Guests, Local account.' **Caution:** Configuring a standalone (non-domain-joined) workstation as described above may result in an inability to remotely administer the workstation. **Note #1:** The security identifier 'Local account' is not available in Windows 7 and Windows 8.0 unless [MSKB 2871997](http://support.microsoft.com/kb/2871997) has been installed. **Note #2:** In all versions of Windows prior to Windows 7, **Remote Desktop Services** was known as **Terminal Services**, so you should substitute the older term if comparing against an older OS.	Follow the Least Privilege Model When Granting RDP Permissions	Supportive Control
18.8.36	18.8.36.1	**(L1) Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'** This policy setting allows you to turn on or turn off Offer (Unsolicited) Remote Assistance on this computer. Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests. The recommended state for this setting is: 'Disabled.'	Follow the Least Privilege Model When Granting RDP Permissions	Supportive Control
18.8.36	18.8.36.2	**(L1) Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'** This policy setting allows you to turn on or turn off Solicited (Ask for) Remote Assistance on this computer. The recommended state for this setting is: 'Disabled.'	Follow the Least Privilege Model When Granting RDP Permissions	Supportive Control
18.9.62.3.3	18.9.62.3.3.2	**(L1) Ensure 'Do not allow drive redirection' is set to 'Enabled'** This policy setting prevents users from sharing the local drives on their client computers to Remote Desktop Servers that they access. Mapped drives appear in the session folder tree in Windows Explorer in the following format: '\\TSClient\<driveletter>$' If local drives are shared they are left vulnerable to intruders who want to exploit the data that is stored on them. The recommended state for this setting is: 'Enabled.'	Protect Data From an RDP-Based Attack	Supportive Control

CIS Benchmark Section #	CIS Benchmark Recommendation #	CIS Benchmark Title and Description	RDP-Related Recommendation	Direct Mitigation or Supportive Control
18.9.62.3.11	18.9.62.3.11.1	**(L1) Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'** This policy setting specifies whether Remote Desktop Services retains a user's per-session temporary folders at logoff. The recommended state for this setting is: 'Disabled.'	Protect Data From an RDP-Based Attack	Supportive Control
2.3.7	2.3.7.2	**(L1) Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'** This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization. The recommended state for this setting is: 'Enabled.'	Protect Data From an RDP-Based Attack	Supportive Control
18.8.4	18.8.4.2	**(L1) Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled'** Remote host allows delegation of non-exportable credentials. When using credential delegation, devices provide an exportable version of credentials to the remote host. This exposes users to the risk of credential theft from attackers on the remote host. The Restricted Admin Mode and Windows Defender Remote Credential Guard features are two options to help protect against this risk. The recommended state for this setting is: 'Enabled.' **Note:** More detailed information on Windows Defender Remote Credential Guard and how it compares to Restricted Admin Mode can be found at this link: [Protect Remote Desktop credentials with Windows Defender Remote Credential Guard (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/access-protection/remote-credential-guard)	Protect Data From an RDP-Based Attack	Supportive Control
18.8.28	18.8.28.1	**(L1) Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'** This policy prevents the user from showing account details (email address or user name) on the sign-in screen. The recommended state for this setting is: 'Enabled.'	Protect Data From an RDP-Based Attack	Supportive Control
17.5	17.5.5	**(L1) Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'** This subcategory reports other logon/logoff-related events, such as Remote Desktop Services session disconnects and reconnects, using RunAs to run processes under a different account, and locking and unlocking a workstation. Events for this subcategory include: 4649: A replay attack was detected. 4778: A session was reconnected to a Window Station. 4779: A session was disconnected from a Window Station. 4800: The workstation was locked. 4801: The workstation was unlocked. 4802: The screen saver was invoked. 4803: The screen saver was dismissed. 5378: The requested credentials delegation was disallowed by policy. 5632: A request was made to authenticate to a wireless network. 5633: A request was made to authenticate to a wired network. The recommended state for this setting is: 'Success and Failure.'	Log and Monitor for RDP-Related Events	Supportive Control

APPENDIX D:
Acronyms

BL	BitLocker Level for CIS Benchmarks
CIA	Confidentiality, Integrity, and Availability
CIFS	Common Internet File System
COM+	Component Object Model Plus
COTS	Commercial-off-the-Shelf
COVID-19	Coronavirus Disease 2019
CredSSP	Credential Security Support Provider
GPME	Group Policy Management Editor
GPO	Group Policy Object
GUI	Graphical User Interface
IDS	Intrusion Detection System
IG	Implementation Group
IT	Information Technology
IP	Internet Protocol
ITU	International Telecommunication Union
ITU T or ITU-T	ITU Telecommunication Standardization Sector
L1	Level 1 for CIS Benchmark
L2	Level 2 for CIS Benchmark
LAN	Local Area Network
LGPE	Local Group Policy Editor
LSP	Local Security Policy
MFA	Multi-Factor Authentication
MSP	Managed Service Provider
MSSP	Managed Security Services Provider
NLA	Network Level Authentication
OS	Operating System
PSO	Password Settings Objects
RCE	Remote Code Execution
RDG	Remote Desktop Gateway
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services (formerly Terminal Services)
SIEM	Security Information and Event Management
SMB	Server Message Block
SME	Small to Medium-Sized Enterprises
SSL	Secure Sockets Layer
TCP/UDP	Transmission Control Protocol/User Datagram Protocol
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

APPENDIX E:
References and Resources

- https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/
- https://docs.microsoft.com/en-us/windows/win32/termserv/remote-desktop-protocol#
- https://enterprise.verizon.com/resources/reports/dbir/
- https://www.cisecurity.org/white-papers/cis-password-policy-guide/
- https://www.cisecurity.org/controls/cis-controls-list/
- https://www.cisecurity.org/cis-benchmarks/
- https://www.microsoft.com/en-us/security/business/security-intelligence-report
  Microsoft Digital Defense Report and Security Intelligence Reports: Get the latest insights about the threat intelligence landscape and guidance from experts, practitioners, and defenders at Microsoft.

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
TheCISecurity
cisecurity