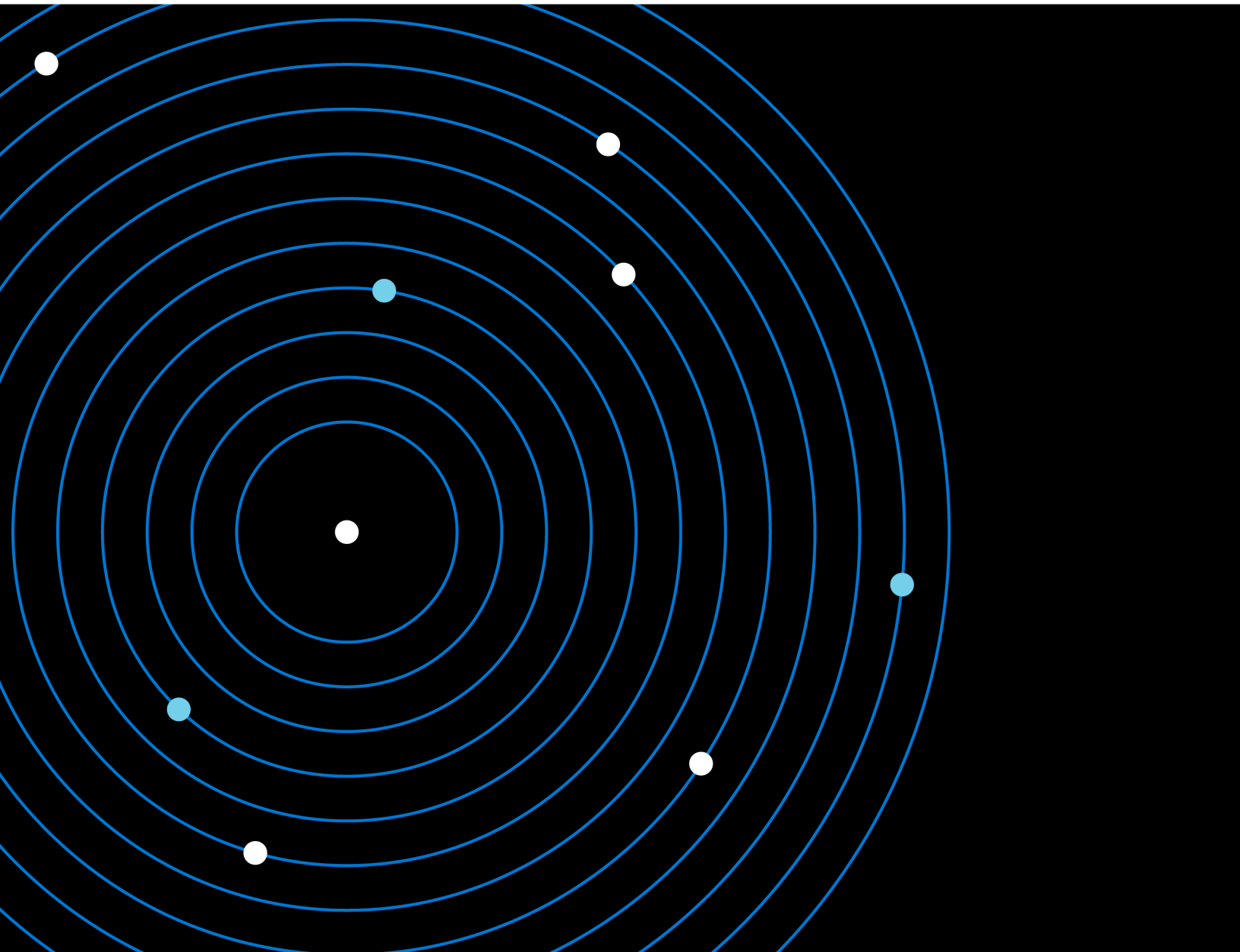
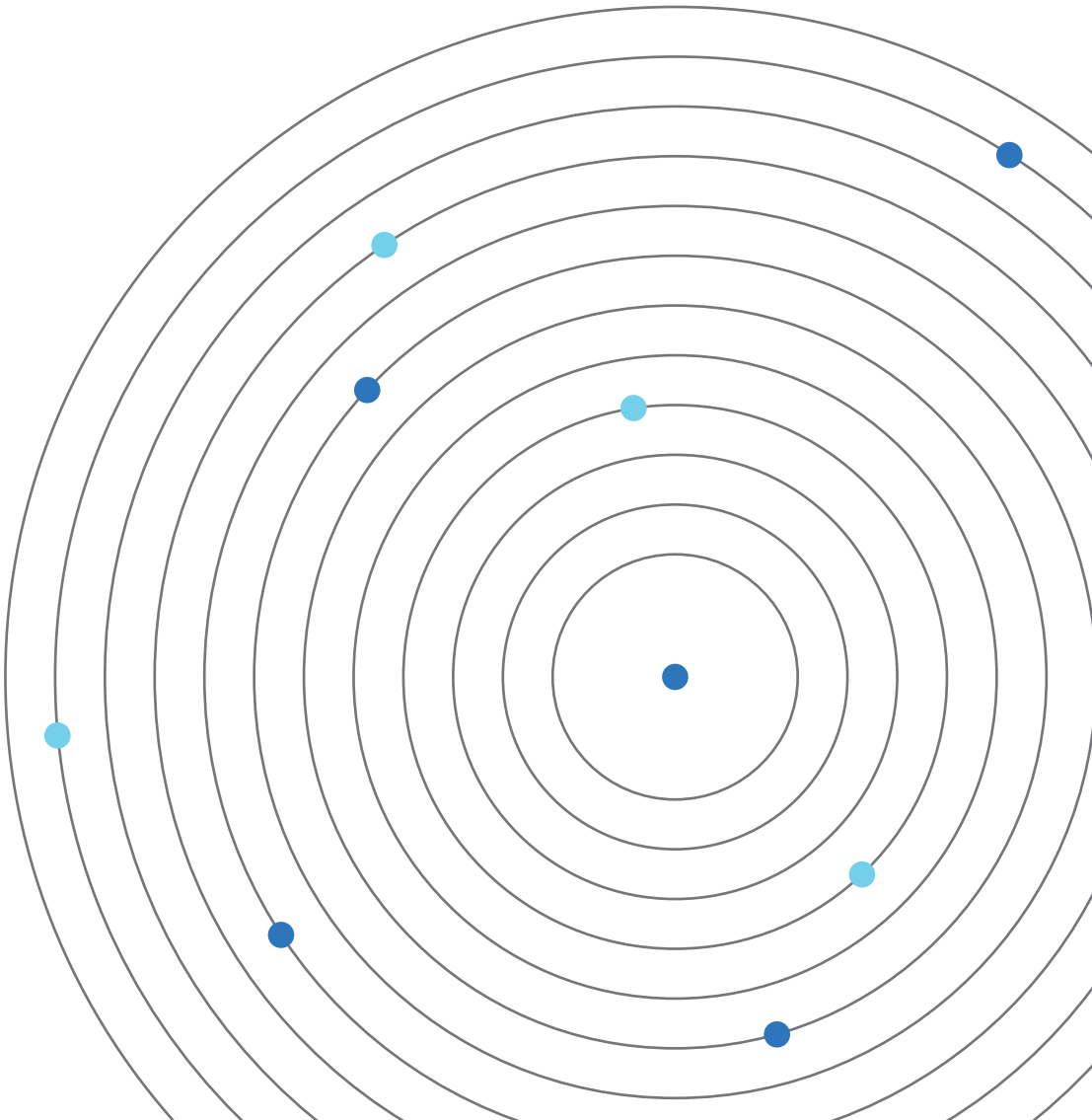
Azure e-book series

Microsoft Azure

Azure Virtual Desktop Handbook: Security Fundamentals



Contents



Introduction

As you progress your journey of enabling remote work for your organization with Azure Virtual Desktop, it is important to understand the security responsibilities, capabilities, and best practices to follow to help keep your users safe.

This handbook guides you through the process of configuring security in your Azure Virtual Desktop environment. Although each section focuses on a specific area and can be implemented independently, we advise reading the complete handbook to inform your end-to-end Azure Virtual Desktop security strategy.

Azure Virtual Desktop overview

Azure Virtual Desktop is a comprehensive desktop and app virtualization service running in the cloud that helps enable a secure remote desktop experience from anywhere, helping organizations strengthen business resilience. It delivers simplified management, Windows 10 multi-session, optimizations for Microsoft 365 Apps for enterprise, and support for migrating Remote Desktop Services (RDS) environments. Azure Virtual Desktop also allows you to deploy and scale your Windows desktops and apps on Azure in minutes and provides built-in security and compliance features to help you keep your apps and data secure.

With Azure Virtual Desktop being based on Platform as a Service (PaaS), many infrastructure-related parts of the solution are managed for you by Microsoft. Other parts, mostly relating to the desktop and application workloads, are managed by the customer or partner.

Figure 1 shows the components joined in four different buckets. The **Azure Virtual Desktop service** and **Azure Infrastructure** buckets are managed by Microsoft. The **Desktop and remote apps** and **Management and policies** buckets are managed by you, which provides you with the full flexibility of being in control of your session host servers and application landscapes.

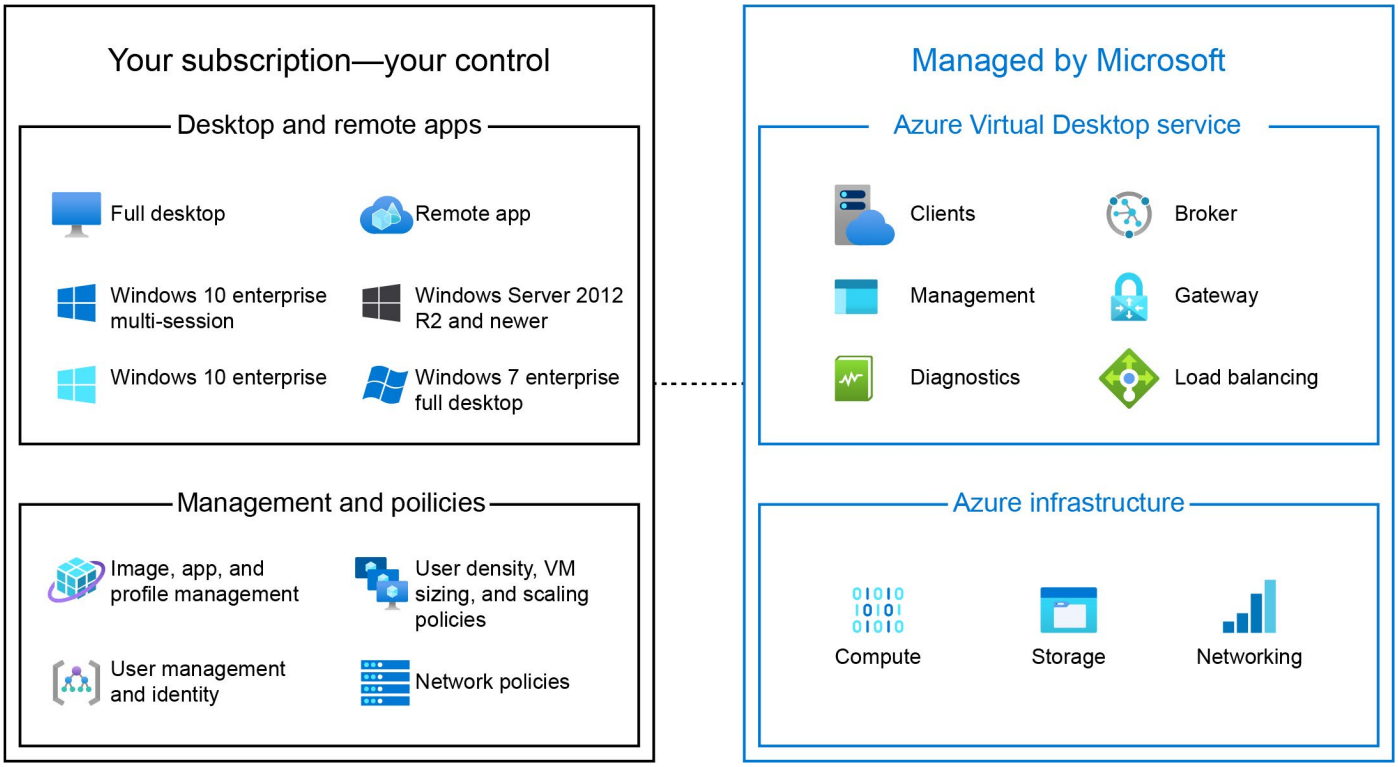


Figure 1: Azure Virtual Desktop component and responsibilities

Figure 2 shows a typical architectural setup of an enterprise environment of Azure Virtual Desktop:

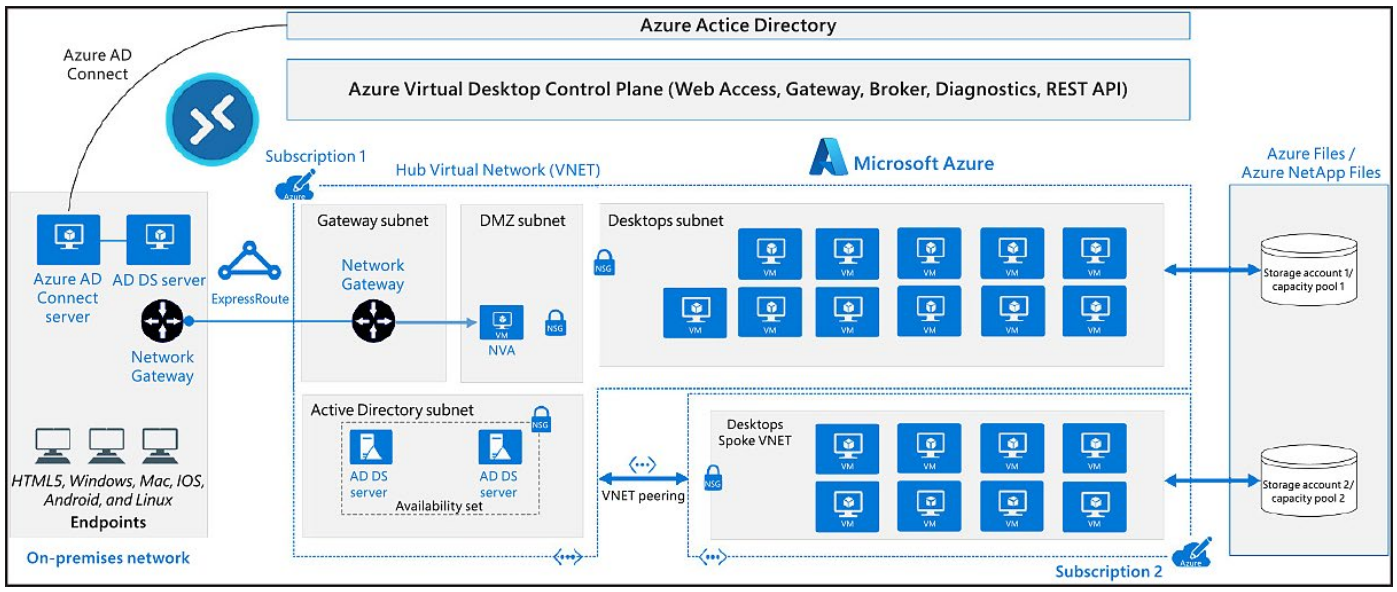


Figure 2: Typical Azure Virtual Desktop architectural setup

The application's back-end components are on the customer's on-premises network. ExpressRoute extends the on-premises network into the Azure cloud. Optionally, the back-end components can also be migrated to Azure as well based on a data center migration scenario. The Azure AD Connect components synchronize identities from Active Directory Domain Services (AD DS) with Azure AD. If Azure Active Directory Domain Services (Azure AD DS) is used, identities will automatically be synchronized from Azure AD to Azure AD DS. The customer manages AD DS and Azure AD, Azure subscriptions, virtual networks, Azure Files or Azure NetApp Files, and the Azure Virtual Desktop host pools and workspaces.

The Azure Virtual Desktop service architecture is similar to that of Windows Server Remote Desktop Services. With Azure Virtual Desktop, however, Microsoft manages the infrastructure and brokering components, while enterprise customers manage their own desktop host virtual machines (VMs), data, and clients. This allows you to shift your focus to what's really important to you, the user experience. To understand the differences between RDS on-premises, migrating to Azure, and migrating to Azure Virtual Desktop, take a look at *Figure 3*:

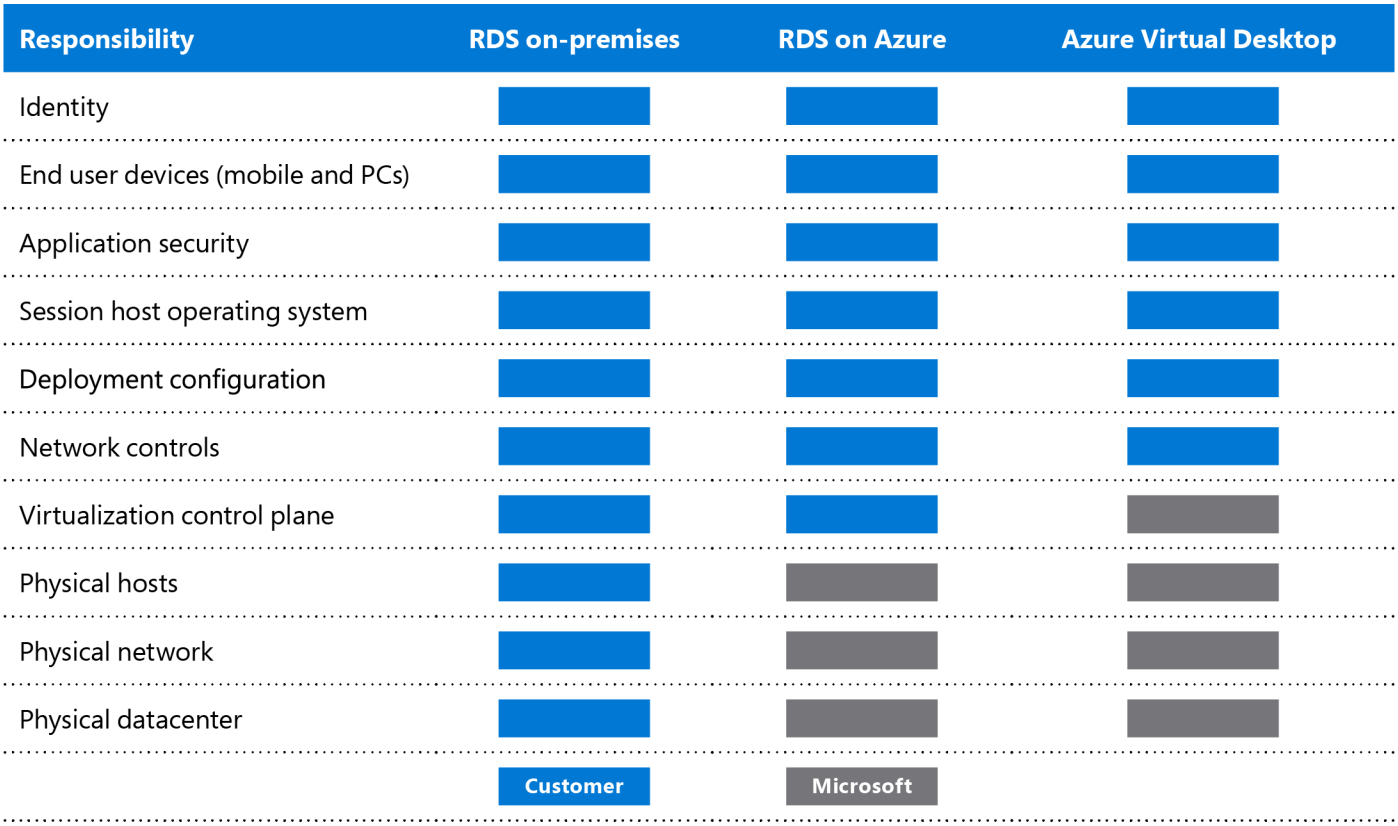


Figure 3: Responsibilities

For more information on Azure Virtual Desktop for the enterprise, visit this page.

Microsoft and customer security responsibilities

Traditionally, when it comes to specific security responsibilities, the customer is responsible for all aspects of security in an on-premises virtual desktop infrastructure (VDI) deployment. With Azure Virtual Desktop, these responsibilities are shared between the customer and Microsoft.

Figure 4 shows how the security responsibilities for Azure Virtual Desktop are divided between Microsoft and the customers:

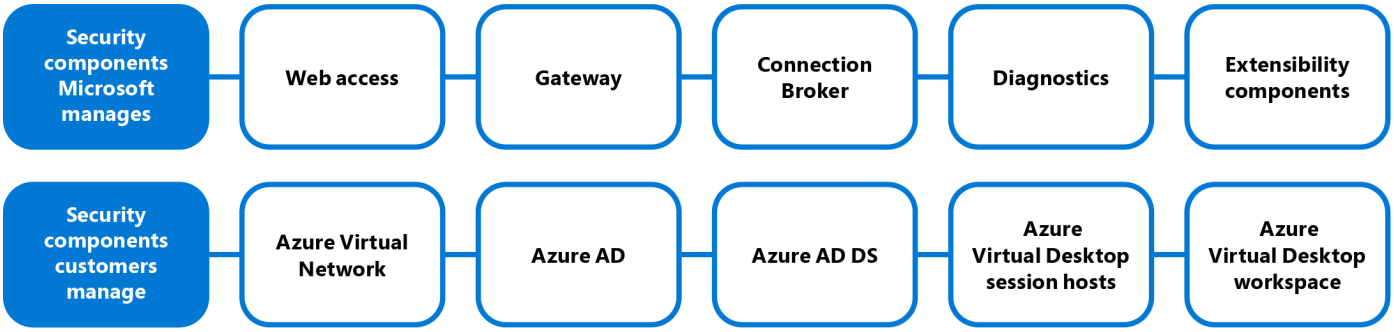


Figure 4: Security component responsibilities

For more information on these components, consult this explanation of the management of Azure Virtual Desktop components.

When you use Azure Virtual Desktop, it's important to understand that Microsoft has already helped secure some services. Microsoft helps secure the physical datacenters, the physical network, and the physical hosts that Azure runs on. Microsoft is also responsible for securing the virtualization control plane, which includes Azure Virtual Desktop services running in Azure. You need to configure other areas to fit your organization's security needs. This handbook provides guidance and best practices to help you configure and optimize the security areas within the services you are responsible for.

Figure 5 shows the different security pillars that are covered in the handbook:

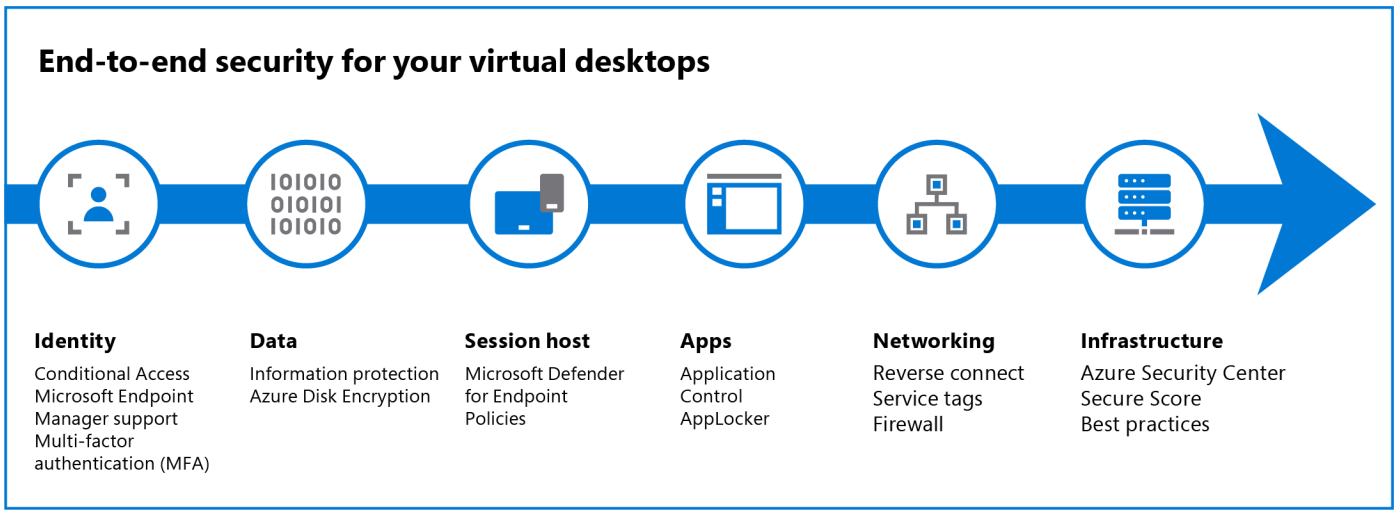


Figure 5: Azure Virtual Desktop Security Information and Event Management

Securing user identities

This chapter guides you through the process of configuring security across the various areas within the Azure Virtual Desktop service. Although each chapter contains a specific area and can be implemented independently, we advise you to read each chapter to familiarize yourself with all the different security aspects.

In this chapter, we address security configurations related to the user's identity. We will discuss user credentials, how to apply Conditional Access, and collecting audit logs.

User credentials

The Windows client for Azure Virtual Desktop is an excellent option for integrating Azure Virtual Desktop with your local machine. However, when you configure your Azure Virtual Desktop account into the Windows client, there are certain measures you will need to take to help you keep yourself and your users safe.

When you first sign in, the client asks for your username and password. After that, the next time you sign in, the client will remember your token from your Azure AD enterprise application. When you select **Remember me** on the prompt for credentials for the session host, your users can sign in after restarting the client without needing to re-enter their credentials. These credentials are stored in the local credential manager. While remembering credentials is convenient, it can also make deployments on enterprise scenarios or personal devices less secure. To help protect your users, you can make sure the client keeps asking for Azure multifactor authentication credentials more frequently by configuring Conditional Access policies for Azure Virtual Desktop.

Conditional Access

Conditional Access is the tool used by Azure AD to bring signals together, make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity-driven control plane. Conditional Access policies at their simplest are if-then statements: if a user wants to access a specific resource, then they must complete one or more actions. By using Conditional Access policies for Azure Virtual Desktop, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when you're not needed. It is all about configuring the correct balance between security and usability. *Figure 6* shows a functional diagram of how Conditional Access works:

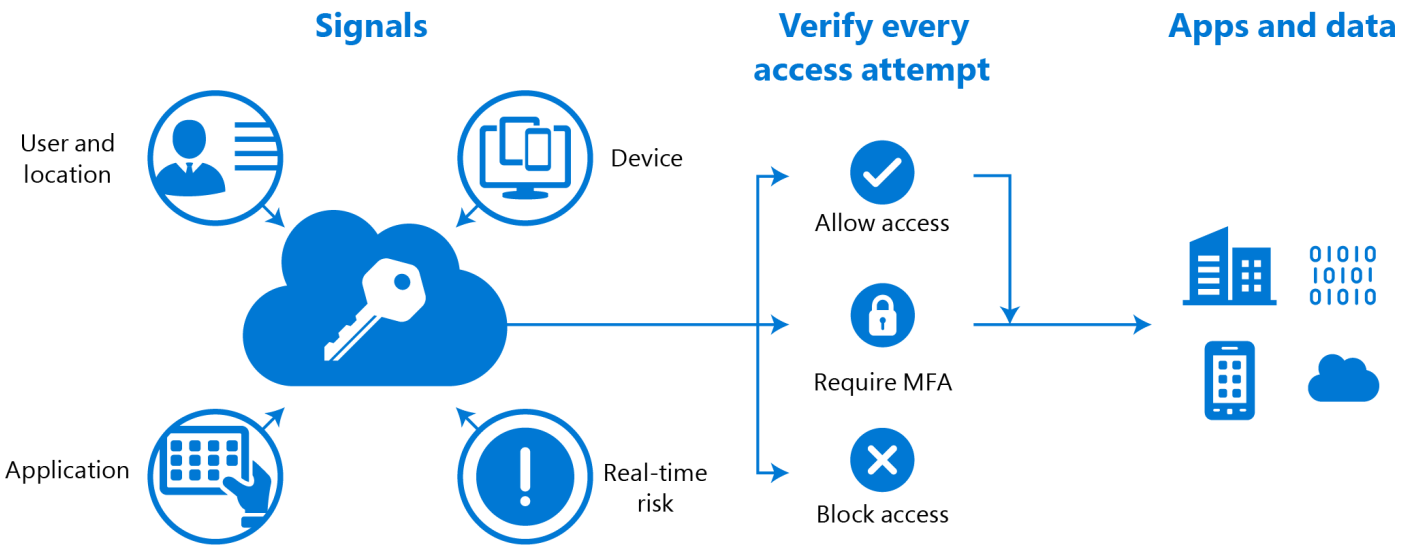


Figure 6: Conditional Access diagram

To get started with Conditional Access and enable Multi-Factor Authentication (MFA) for Azure Virtual Desktop, you need to:

- Assign users a license that includes Azure AD Premium P1 or P2.
- Have an Azure AD group with your users assigned as group members.
- Enable Azure multifactor authentication for all your users.

To configure Conditional Access:

- Sign in to the Azure portal as a global administrator, security administrator, or Conditional Access administrator and browse to **Azure Active Directory** > **Security** > **Conditional Access** and select **New policy**.
- Give your policy a name and under **Assignments**, select **Users and groups** and assign a previously created group.
- Under **Cloud apps or actions** > **Include**, select **Select apps** and then select **Azure Virtual Desktop** (App ID 9cdead84-a844-4324-93f2-b2e6bb768d07).
- Now go to **Conditions** > **Client apps** and then select where you want to apply the policy. This can either be **Browser** (for the Azure Virtual Desktop Web Client), **Mobile apps and desktop clients**, or both.
- Under **Access controls** > **Grant**, select **Grant access**, select **Require multi-factor authentication**, and then select **Select**.
- Under **Access controls** > **Session**, select **Sign-in frequency**, set the value to the time you want between prompts, and then click on **Select**.
- And finally, confirm your settings and set **Enable policy** to **On**. The policy will look like *Figure 7*:

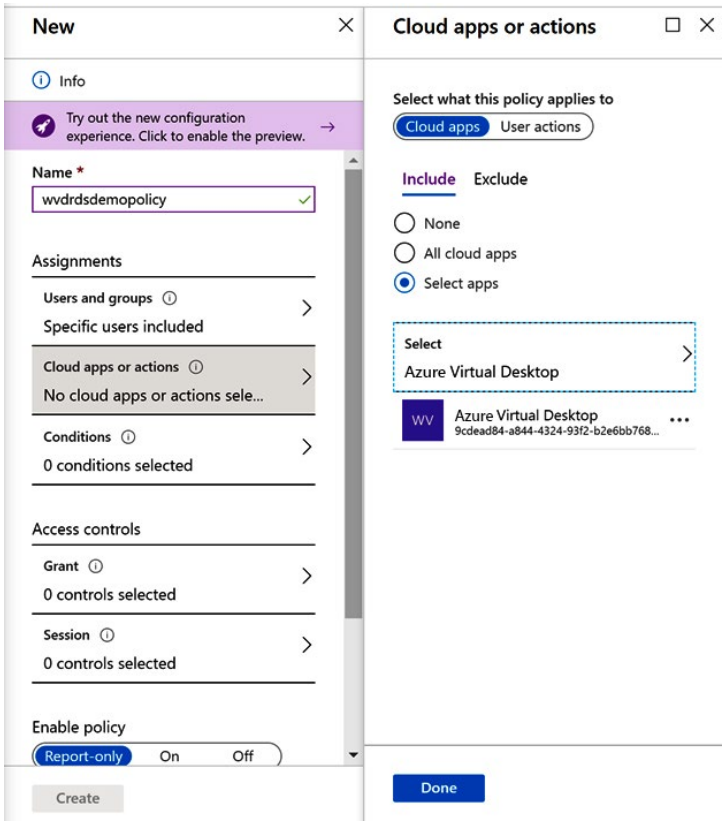


Figure 7: MFA configuration for Azure Virtual Desktop

You have now configured a basic Conditional Access policy that enforces MFA for a specific group and specific Azure Virtual Desktop client with a configured sign-in frequency.

For more information, read this article, which covers enabling Azure multifactor authentication for Azure Virtual Desktop in greater detail. And finally, the sign-in frequency that we configured within the Conditional Access policy defines the time period before a user is asked to sign in again when attempting to access a resource. Consult this guide for more information on User sign-in frequency.

Collecting audit logs

When it comes to securing user identities, collecting and examining audit logs is important too. With audit log collection enabled, you collect and gain insights into user as well as admin activities related to Azure Virtual Desktop. The following list provides you with six example areas to get you started with collecting audit logs for Azure Virtual Desktop:

- Azure Activity Log
- Azure Active Directory Activity Log
- Azure Active Directory
- Session hosts
- Azure Virtual Desktop Diagnostic Log
- Key Vault logs

Securing data

When providing users access to your Azure Virtual Desktop environment, you also allow them to store and access personal data as part of their user profile. This chapter discusses how to help secure that data.

FSLogix profile containers

A user profile is a collection of configurations that represents the state of a system. There are various system components that bind to a user's profile. These components include applications, registry entries, and other customized entries. Windows 10 offers several types of user profiles, but we recommend using FSLogix Profile Containers to store the whole user profile. Profile containers redirect the entire user profile to a remote location and are therefore not a traditional profile management solution. There are three common ways to store these profile containers:

- Profile containers using a file share, based on Storage Spaces Direct
- Profile containers using Azure Files and Azure AD DS or Azure Files and AD DS
- Profile containers using Azure NetApp Files and AD DS

We recommend storing FSLogix profile containers on Azure Files or Azure NetApp Files instead of using file shares for most of our customers, but for more details on the differences, consult the storage options comparison article.

Azure Disk Encryption

Using Azure Files as the solution for profile containers supports Server Message Block (SMB) identity-based authentication by using on-premises AD DS with Azure AD DS. Azure Files applies Kerberos protocols for authenticating with either on-premises AD DS or Azure AD DS.

With Azure NetApp Files, all files that Azure Virtual Desktop uses are encrypted through the Federal Information Processing Standards Publications (FIPS PUBS) 140-2 standard. The Azure NetApp Files service manages all keys and generates a unique XTS-AES-256 data encryption key for each volume. Azure Virtual Desktop uses an encryption key to encrypt and help you protect all volume keys. In an encrypted format, encryption keys are unavailable or reported. The keys are also deleted immediately when a volume is deleted.

When it comes to security and compliance, both Azure Files and Storage Spaces Direct have all Azure-supported certificates. Azure NetApp Files is ISO complete. To learn more about FSLogix profile containers, user profile disks, and other user profile technologies, see the table in FSLogix profile containers and Azure files.

To start creating your own FSLogix profile containers setup, get started with one of these tutorials:

- Create a profile container with Azure Files and AD DS.
- Create a profile container with Azure NetApp Files and AD DS.
- Create a profile container by using a file share.

Securing session hosts and applications

You can take several actions and use multiple tools to help secure your Azure Virtual Desktop session hosts and applications. This chapter discusses what you can do to secure those components of your Azure Virtual Desktop environment.

Microsoft Defender for Endpoint

To help secure your endpoints against malware and advanced threats, we recommend that you configure Microsoft Defender for Endpoint, previously known as Microsoft Defender Advanced Threat Protection. There are multiple ways to deploy Microsoft Defender for Endpoint on your Azure Virtual Desktop VMs. You can use a local group policy, a domain group policy, and also onboard using management tools. For more guidance, follow this article that explains how to Onboard Windows 10 multi-session devices in Azure Virtual Desktop. Single-session scenarios on Windows 10 Enterprise and Windows 10 Enterprise multi-session are both fully supported, and onboarding your Azure Virtual Desktop machines into Defender for Endpoint has not changed. Previously, there was a soft limit for Defender for Endpoint supporting up to 50 concurrent user connections for Windows 10 Enterprise multi-session, but this soft limit has been removed. When using Windows 10 Enterprise multi-session, depending on your requirements, you can choose to either have all users licensed through Microsoft Defender for Endpoint (per user), Windows Enterprise E5, Microsoft 365 Security, or Microsoft 365 E5, or have the VM licensed through Azure Defender. Read this article for more information on Microsoft Defender for Endpoint capabilities for Azure Virtual Desktop.

Microsoft Endpoint Manager integration with Microsoft Intune

You can use Microsoft Intune to create and check policies for compliance. You can also use it to deploy applications, features, and settings to your devices that run on Azure. For guidance, follow the tutorial Walkthrough Intune in Microsoft Endpoint Manager. Microsoft Intune is also integrated with Azure AD for authentication and authorization. It also integrates with Azure Information Protection for data protection. You can use Microsoft Intune with the Microsoft 365 suite of products. Application control moves from an application trust model that assumes all applications

are trustworthy. The new model demands that applications earn trust before they can run. Microsoft Defender Application Control and AppLocker are included in Windows 10 for providing application control and can also be used as security methods in Azure Virtual Desktop environments. We will discuss these two methods in the upcoming paragraphs in more detail.

Windows Defender Application Control

With thousands of new malicious files created every day, using traditional methods like antivirus solutions—signature-based detection to fight against malware—provides an inadequate defense against new attacks. Windows Defender Application Control can help mitigate these types of security threats by restricting the applications that users are allowed to run and the code that runs in the system core (kernel). Application Control was introduced with Windows 10 and, with Azure Virtual Desktop, allows you to control which drivers and applications are allowed to run on your Azure Virtual Desktop hosts. Application Control was designed as a security feature under the servicing criteria defined by the Microsoft Security Response Center (MSRC). For more information on which individual Application Control features are available on which Application Control builds, see feature availability documentation. Visit this page to get started with Application Control.

AppLocker

AppLocker helps to prevent users from running unapproved software. AppLocker control policies restriction rules are based on file attributes, product names, file names, or file versions. AppLocker includes default rules for each rule collection to ensure that the files required for Windows to operate properly are allowed in an AppLocker rule collection. The default rules also allow members of the local administrators group to run all Windows Installer files. An AppLocker rule collection functions as an allowed list of files. Only the files that are listed in the rule collection can run. This configuration makes it easier to determine what will occur when an AppLocker rule is applied. Because AppLocker functions as an allowed list by default, if no rule explicitly allows or denies a file from running, AppLocker's default deny action will block the file. Although AppLocker is a very powerful tool, generally, it is recommended that if you are able to implement application control using Application Control rather than AppLocker, do so.

Application Control is undergoing continuous improvements and will be getting added support from Microsoft management platforms. Although AppLocker will continue to receive security fixes, it will not undergo new feature improvements. In some cases, however, AppLocker may be the more appropriate technology for your organization. For example, when you have mixed Windows operating system (OS) environments, you need to apply different policies for different users or groups on a shared computer or you do not want to enforce application control on application files such as DLLs or drivers. As a best practice, you should enforce Application Control at the most restrictive level possible for your organization, and then you can use AppLocker to further fine-tune the restrictions. Visit this page to get started with AppLocker.

The Application Control and AppLocker feature availability matrix provides a more detailed comparison of the two technologies.

FSLogix Application Masking

The primary use case for Application Masking is to significantly decrease the complexity of managing large numbers of golden images (master images). Although not primarily intended as a security measure, Application Masking can also be used to provide security for applications. Application Masking manages access to applications, fonts, and other items based on criteria. The Application Rules Editor is used to describe the item, such as an application, to be managed. Application Masking may be used in both physical and virtual environments. Application Masking is most often applied to manage non-persistent, virtual environments, such as virtual desktops. To get started with Application Masking, follow the tutorial Implement FSLogix Application Masking.

Screen capture protection

The screen capture protection (preview) feature prevents sensitive information from being captured on the client endpoints. When you enable this feature, remote content will be automatically blocked or hidden in screenshots and screen shares. It will also be hidden from malicious software that may be continuously capturing your screen's content. When using this feature, we recommend that you also disable clipboard redirection (discussed in this handbook later on) to prevent the copying of remote content to endpoints while using this feature. This policy is enforced at the host level by configuring a registry key. To enable this policy, open PowerShell and set the fEnableScreenCaptureProtection registry key:

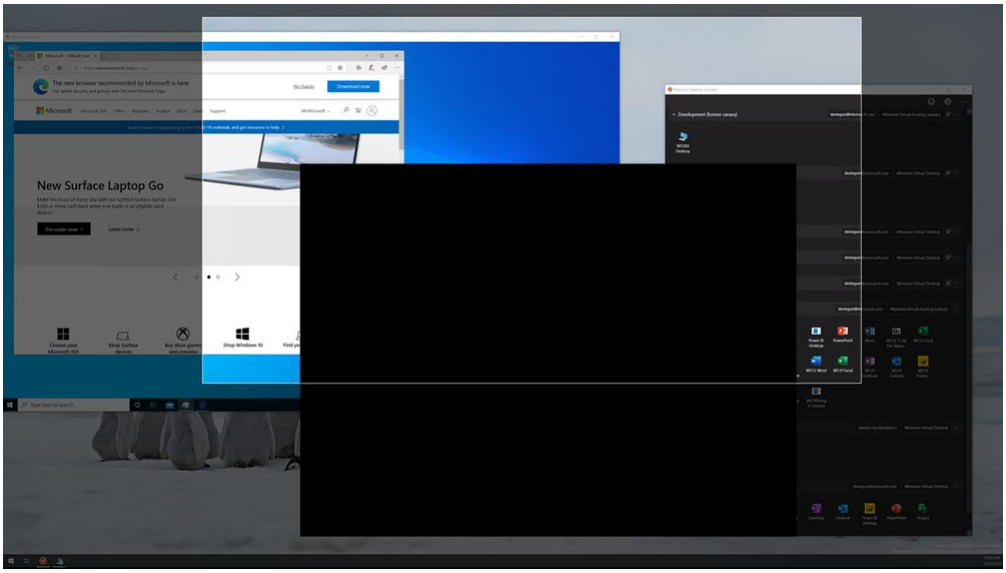


Figure 8: An example of the screen capture protection feature

To test this new feature, your host pools need to be provisioned in a validation environment and you need to have downloaded and installed the Windows Desktop client, version 1.2.1526 or later. The feature of course does not prevent users from taking pictures of their screen, for example, by using their cellphones. However, it does provide you with the option to add an additional layer of security.

For more detailed instructions on enabling screen capture protection, visit this page.

Patching software in your environment

Once you identify a vulnerability in any environment, you must patch it as soon as possible. This applies to Azure Virtual Desktop environments as well. This includes the running operating systems, the applications that are deployed inside of them, and the images you create new machines from. Follow your vendor patch notification communications and apply patches in a timely manner. We recommend patching your base images monthly to ensure that newly deployed machines are as secure as possible.

For more information, follow the guide to Prepare and customize a master VHD image.

Master images typically, besides predefined security, also include necessary software and configuration settings. Setting up your own imaging pipeline requires time and infrastructure. With Azure VM Image Builder, you just provide a simple configuration describing your image, submit it

to the service, and the image is built and distributed. Azure Image Builder is a fully managed Azure service that is accessible by an Azure resource provider. The Azure Image Builder process has three main parts: source, customize, and distribute; they are represented in a template.

Figure 9 shows the Image Builder process. The result of the Azure Image Builder process is a template image, stored as a Virtual Hard Disk (VHD) managed image inside a Shared Image Gallery, which can then be used to (re)build your Azure Virtual Desktop session hosts.

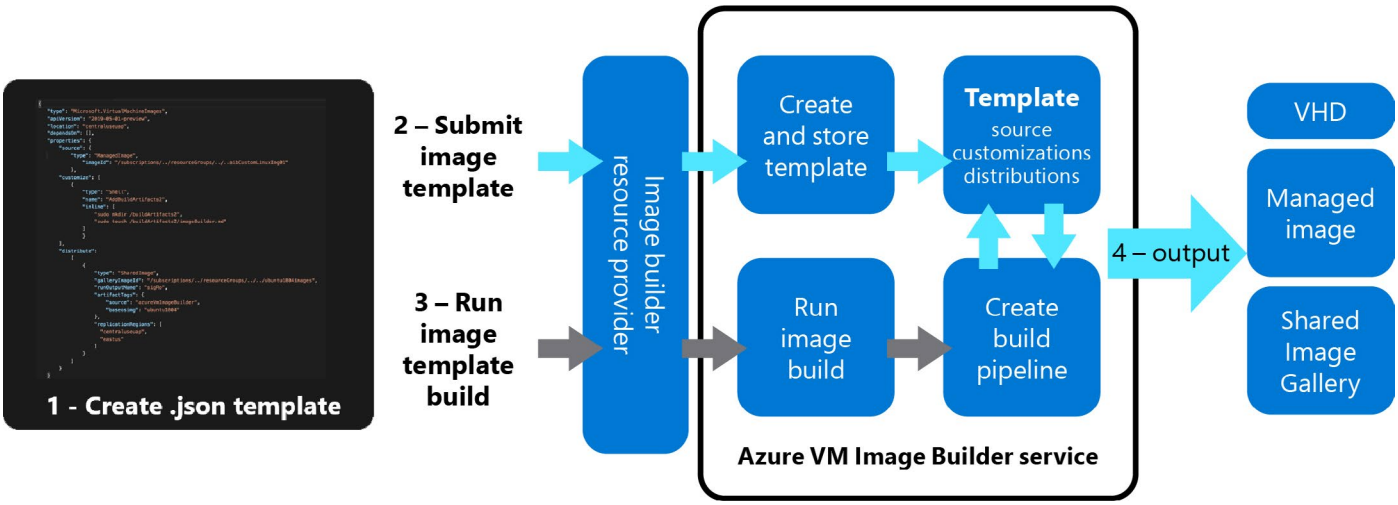


Figure 9: Azure Image Builder process

For more information, consult the Azure Image Builder overview.

Maximum inactive/disconnection time policies and screen locks

Signing users out when they are inactive preserves resources and prevents access by unauthorized users. We recommend that timeouts balance user productivity as well as resource usage. For users that interact with stateless applications, consider more aggressive policies that turn off machines and preserve resources. Disconnecting long-running applications that continue to run if a user is idle, such as a simulation or CAD rendering, can interrupt the user's work and may even require restarting the computer. You can also prevent unwanted system access by configuring Azure Virtual Desktop to lock a machine's screen during idle time and requiring authentication to unlock it. Maximum inactive/disconnection time can be configured inside the template image using the Local Group Policy Editor, or centrally using Group Policy Objects. *Figure 10* shows the location of the various settings.

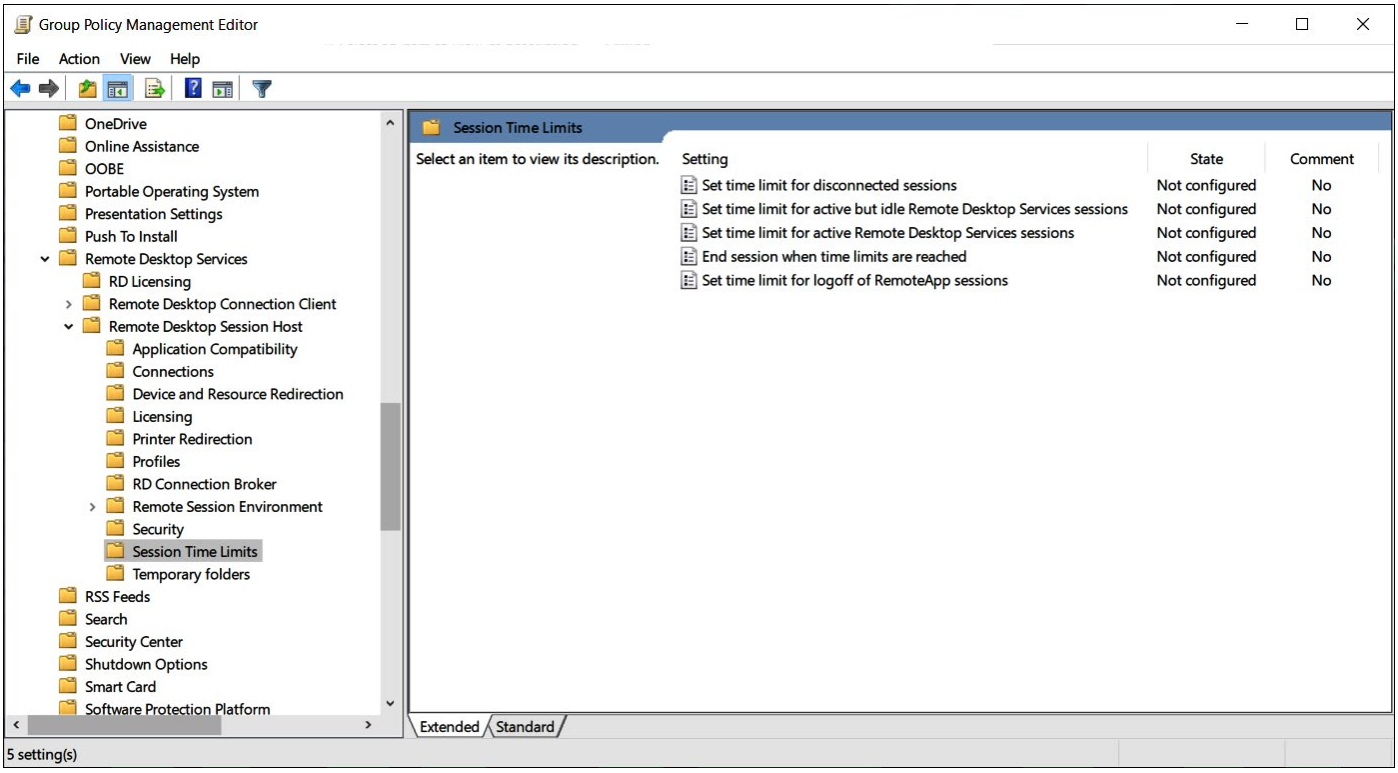


Figure 10: Group Policy location for session limits

Configuring device redirection

Users can bring a wide variety of different (peripheral) devices to their Azure Virtual Desktop session. Although this is a great feature that significantly improves the overall user experience, make sure you choose wisely what you allow users to redirect. For example, you might not want users to copy clipboard data from their Azure Virtual Desktop session to their local client, or you might want to prevent access to USB drives within Azure Virtual Desktop. We recommend that you evaluate your security requirements and check if these features should be disabled or not.

Figure 11 shows some of the options that can be changed as part of the RDP properties of the host pool. At the Azure Virtual Desktop page, select Host pools in the menu on the left side of the screen, then select RDP Properties in the menu on the left side of the screen. Alternatively, you can open the Advanced tab and add your RDP properties in a semicolon-separated format. When you are done, select Save to save your changes.

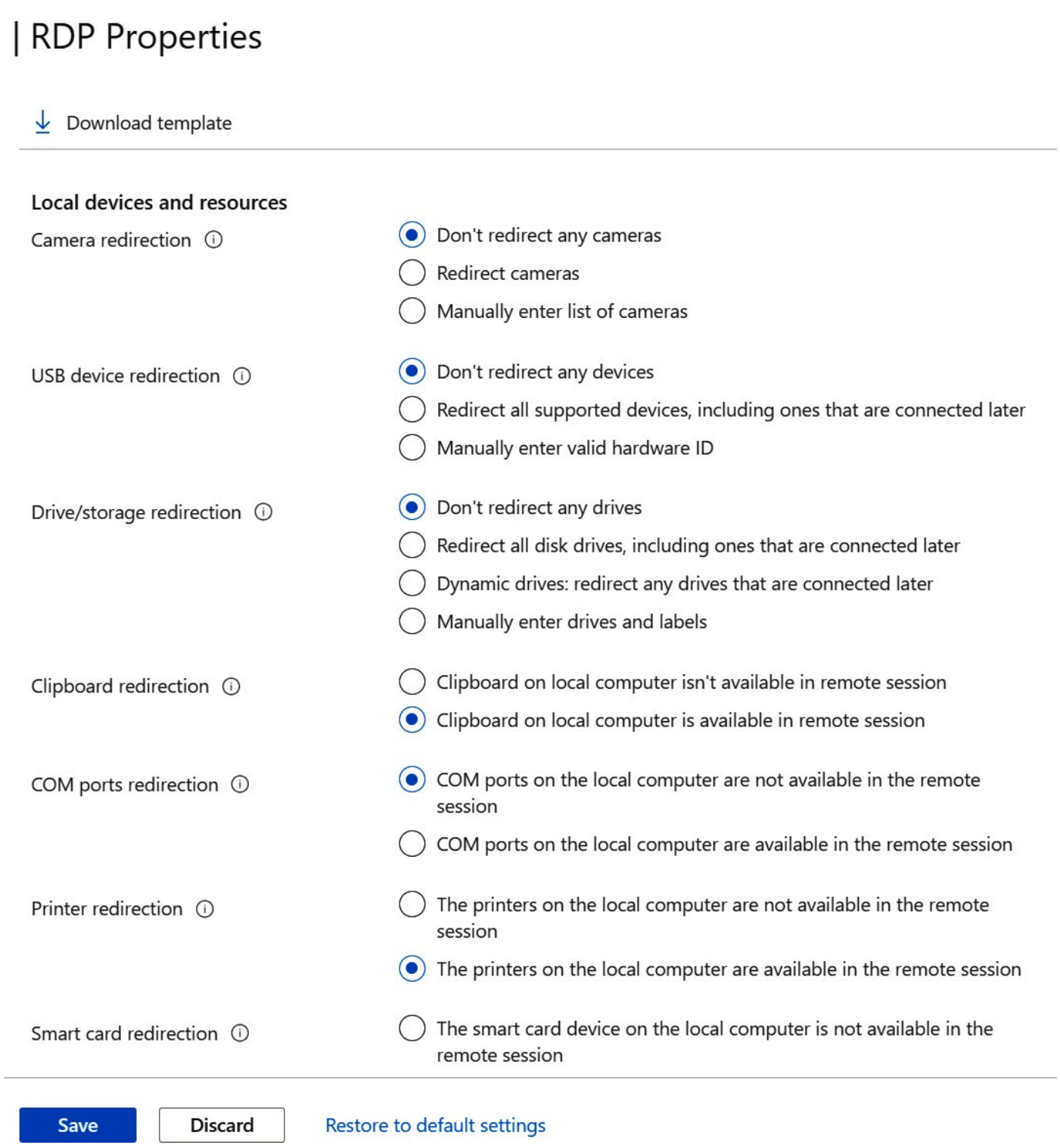


Figure 11: Options for the RDP properties of the host pool

To learn more, follow this guide, which provides detailed information about customizing Remote Desktop Protocol (RDP) properties for a host pool.

Restricting Windows Explorer access

In most Azure Virtual Desktop deployments, pooled scenarios are implemented because this provides a better cost optimization. It essentially means users share Azure VM resources by logging in to a session host with multiple users at the same time. As a result, it is recommended to perform lockdown policies so that users cannot access each other's session data or perform unwanted actions on the shared VM. Restricting Windows Explorer access by hiding local and remote drive mappings prevents users from discovering unwanted information about system configuration and users. Configuring these settings can be performed within the template image but can also be applied using Group Policy Objects.

Figure 12 shows the Group Policy Object location that can be used to configure Windows Explorer access.

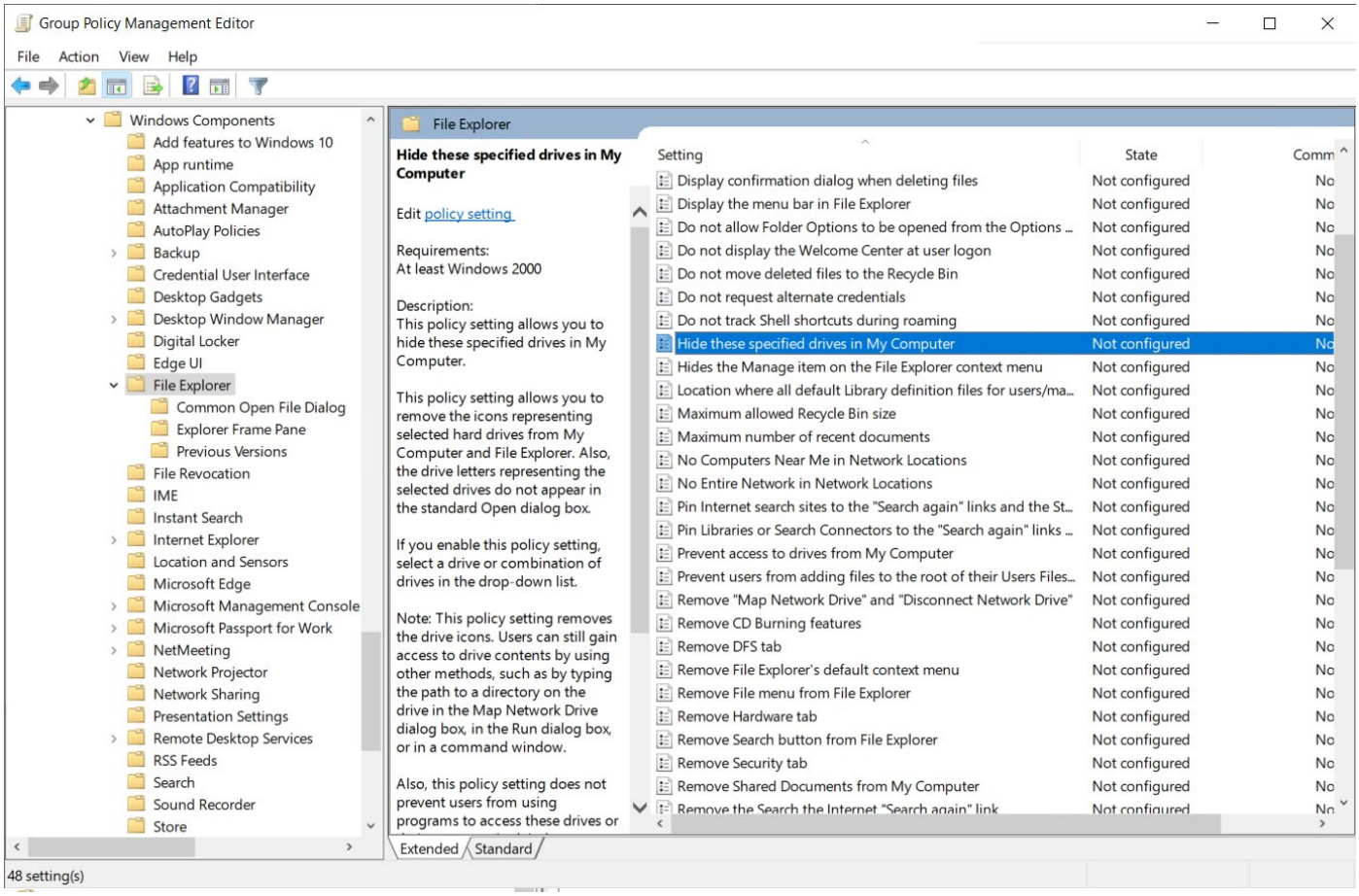


Figure 12: The Group Policy Object location for configuring Windows Explorer access

For more information about restricting Windows Explorer access by hiding drives, check out the tutorial Using Group Policy Objects to hide specified drives. Note that hiding a drive does not prevent access. Optionally, you can also prevent access to specific drives. In general, investigate settings to further lock down the session host, for example, by preventing access to Command Prompt, the Control Panel, or Windows settings. Discussing all of these settings in great detail goes beyond the scope of this handbook.

Managing Microsoft 365 Apps security

In addition to securing your session hosts themselves, it is also important to secure the applications running inside them. Microsoft 365 Apps (previously Microsoft Office Pro Plus) are some of the most common applications we see deployed in session hosts. To improve the Office deployment security, we recommend you use the Security Policy Advisor for Microsoft 365 Apps for enterprise. This tool identifies policies you can apply to your deployment to add more security. Security Policy Advisor also recommends policies based on their impact on your security and productivity. When a security group has been assigned a policy configuration, Security Policy Advisor analyzes how users in that group work with Microsoft 365 Applications. Based on this analysis and on Microsoft best practices, recommendations are created for specific security policies and insights about the impact of those policies on productivity and security. For more information, consult this Overview of Security Policy Advisor for Microsoft 365 Apps for enterprise.

Securing network access

Azure Virtual Desktop uses Remote Desktop Protocol (RDP) to provide remote display and input capabilities over network connections. The connection data flow for Azure Virtual Desktop starts with a DNS lookup for the closest Azure datacenter. The gateway acts as an intelligent reverse proxy. The gateway manages all session connectivity, with nothing but pixels reaching the client. There are five steps that make up a user connection:

1. When authenticated in Azure AD, a token is returned to the Remote Desktop Services client.
2. The gateway checks the token with the connection broker.
3. The broker queries the Azure SQL Database for resources assigned to the user.
4. The gateway and the broker select the session host for the connected client.
5. The session host creates a reverse connection to the client by using the Azure Virtual Desktop gateway.

Figure 13 shows the five-step connection process for Azure Virtual Desktop running in Azure:

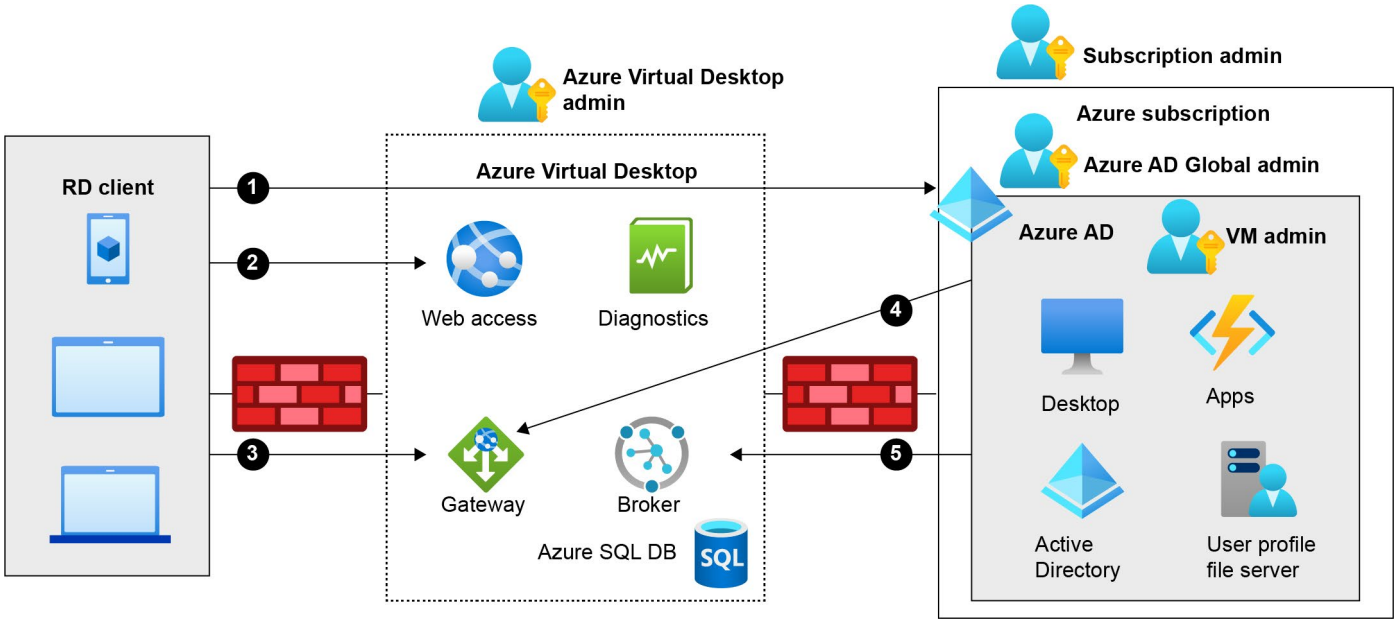


Figure 13: Five-step connection process for Azure Virtual Desktop

TLS 1.2 is used for all connections initiated from the clients and session hosts to the Azure Virtual Desktop infrastructure components. Azure Virtual Desktop uses the same TLS 1.2 ciphers as Azure Front Door. It is important to make sure both client computers and session hosts can use these ciphers. For reverse connect transport (further explained in the next paragraph), both the client and the session host connect to the Azure Virtual Desktop gateway. After establishing the TCP connection, the client or session host validates the Azure Virtual Desktop gateway's certificate. After establishing the base transport, RDP establishes a nested TLS connection between the client and the session host using the session host's certificates.

Reverse connect

If you are familiar with Remote Desktop Services (RDS), and Remote Desktop Gateway (RD Gateway) in particular, you will know that in order to allow the user to connect to a Remote Desktop Session Host (RD Session Host), TCP port 3389 has to be open from the RD Gateway toward the RD Session Host.

Unlike RDS, Azure Virtual Desktop by default adds an additional layer of security and as a result does not need a TCP listener to receive incoming RDP connections. Azure Virtual Desktop uses reverse connect transport for establishing the remote session as well as for carrying the RDP traffic. The Azure Virtual Desktop Agent that is automatically installed on the session host is configured to use outbound connectivity to the Azure Virtual Desktop infrastructure over the HTTPS connection. As a result, no inbound ports are needed inside the firewall in front of the session hosts. There is no additional action needed to enable Reverse Connect, but we advise you to make sure you do not have TCP port 3389 open unnecessarily.

In general, avoid direct RDP access to session hosts in your environment. If you need direct RDP access for administration or troubleshooting, connect from an internal network, or enable just-in-time access to limit the potential attack surface on a session host.

Network security group service tags

Another security measure you can take is limiting Azure Virtual Desktop traffic with network security group (NSG) service tags.

Service tags simplify security for Azure VMs. Because Azure virtual networks are used in a Azure Virtual Desktop deployment, service tags make it easy to restrict network access to just the Azure services. You can use service tags in your NSG rules to allow or deny traffic to a specific Azure service globally or per Azure region. An NSG is a collection of security rules that grant or deny network traffic flow into or out of Azure resources. Each rule can specify the following properties: name, priority, source or destination, protocol, direction, port range, and action. NSGs are a layer 3 and layer 4 network security service.

The Azure VMs you create for Azure Virtual Desktop must have access to several Fully Qualified Domain Names (FQDNs) to function properly. The following table shows these FQDNs and ports:

Address	Outbound TCP port	Purpose	Service Tag
*.wvd.microsoft.com	443	Service traffic	WindowsVirtualDesktop
gcs.prod.monitoring.core.windows.net	443	Agent traffic	AzureCloud
production.diagnostics.monitoring.core.windows.net	443	Agent traffic	AzureCloud
*xt.blob.core.windows.net	443	Agent traffic	AzureCloud
*eh.servicebus.windows.net	443	Agent traffic	AzureCloud
*xt.table.core.windows.net	443	Agent traffic	AzureCloud
*xt.queue.core.windows.net	443	Agent traffic	AzureCloud
catalogartifact.azureedge.net	443	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Windows activation	Internet
mrsglobalsteus2prod.blob.core.windows.net	443	Agent and SXS stack updates	AzureCloud
wvdportalstorageblob.blob.core.windows.net	443	Azure portal support	AzureCloud
169.254.169.254	80	Azure Instance Metadata service endpoint	N/A
168.63.129.16	80	Session host health monitoring	N/A

Azure Firewall for application-level protection

Azure Firewall provides a Azure Virtual Desktop FQDN tag to simplify the configuration, as explained previously. Use the following steps to allow outbound Azure Virtual Desktop platform traffic using Azure Firewall:

- Deploy Azure Firewall and configure your Azure Virtual Desktop host pool subnet User Defined Route (UDR) to route all traffic via Azure Firewall.
- Create an application rule collection and add a rule to enable the AzureVirtualDesktop FQDN tag.
- The set of required storage and service bus accounts for your Azure Virtual Desktop host pool is deployment specific, so it is not yet captured in the AzureVirtualDesktop FQDN tag. Address this by allowing HTTPS access from your host pool subnet to *xt.blob.core.windows.net, *eh.servicebus.windows.net, and *xt.table.core.windows.net. These wildcard FQDNs enable the required access but are less restrictive. The other option is to use a log analytics query to list the exact required FQDNs and then allow them explicitly in your firewall application rule.
- Create a network rule collection and allow traffic from your AD DS private IP address to * for TCP and UDP ports 53 and allow traffic from your Azure Virtual Desktop VMs to Windows Activation Service TCP port 1688.

More detailed information about this configuration can be found in the guide Host pool outbound access to Azure Virtual Desktop.

Host pool outbound access to the internet

Depending on your use case, you may need to enable secure outbound internet access for your users. In cases where the list of allowed destinations is well defined (for example, Microsoft 365 access), you can use Azure Firewall application and network rules to configure the required access. In the case of applications that are less well defined, it may be more work to whitelist these destinations. You can of course also configure web browsers or other applications running on the Azure Virtual Desktop host pool with an explicit proxy configuration if you want to filter outbound user internet traffic using an existing on-premises secure web gateway.

Azure security best practices

In this section, we provide generic guidance on providing security using Azure Security Center, improving your security score, and using the Azure security baseline for Azure Virtual Desktop.

Azure Security Center

Azure Security Center provides free security posture management capabilities with Secure Score and threat protection capabilities with the integration of Azure Defender.

In general, we recommend monitoring your Secure Score to strengthen the overall security of your environment, including Azure Virtual Desktop. To get started, follow this quickstart guide to set up Azure Security Center.

Secure Score provides recommendations and best practice advice for improving your overall security. These recommendations are prioritized to help you pick which ones are most important, and the Quick Fix options help you address potential vulnerabilities quickly. These recommendations also update over time, keeping you up to date on the best ways to maintain your environment's security. To learn more, see Improve your Secure Score in Azure Security Center.

Once you start monitoring your security posture, we recommend enabling Azure Defender to protect your hybrid cloud workloads such as VMs, SQL, storage accounts, containers, and key vaults. With Azure Defender, you can get a prioritized view of your threat alerts, manage vulnerabilities, and assess compliance with common frameworks like PCI.

Security alerts can be managed from the Azure Defender portal, and they can also be exported to your Security Information and Event Management (SIEM) tool to perform analysis and remediation. Microsoft's cloud SIEM tool is called Azure Sentinel. Integrating Azure Security Center with Azure Sentinel is extremely beneficial for your Security Operations Center.

Azure Sentinel is a cloud-native SIEM tool that provides intelligent security analytics across your entire organization, collecting data across all users, data, applications, and infrastructure. Azure Sentinel uses AI and machine learning to make threat detection smarter and faster, and its cloud-native nature eliminates the cost, infrastructure, and maintenance demanded by traditional SIEM tools. Especially for Azure Virtual Desktop, Azure Sentinel can ingest Windows event logs from your session hosts, Microsoft Defender for Endpoint alerts, and also Azure Virtual Desktop diagnostics. The latter is a feature of the Azure Virtual Desktop service that logs information whenever someone is assigned a Azure Virtual Desktop role and uses the service.

More information is also provided in the article that discusses how to use Log Analytics for the diagnostics feature for Azure Virtual Desktop.

Azure security baseline for Azure Virtual Desktop

The Azure security baseline for Azure Virtual Desktop applies guidance from the Azure Security Benchmark version 2.0 to Azure Virtual Desktop. It provides recommendations on how you can secure your cloud solutions on Azure. The content of the Azure security baseline for Azure Virtual Desktop is easily grouped by the security controls defined by the Azure Security Benchmark and the related guidance applicable to Azure Virtual Desktop.

The following table provides direct links to the topics covered in the baseline:

Azure security baseline for Azure Virtual Desktop
NS - Network Security
IM - Identity Management
PA - Privileged Access
DP - Data Protection
AM - Asset Management
LT - Logging and Threat Detection
IR - Incident Response
PV - Posture and Vulnerability Management
ES - Endpoint Security
BR - Backup and Recovery
GS - Governance and Strategy

Conclusion

Summary

We started this handbook with an introduction to the importance of securing your Azure Virtual Desktop environment and covered the high-level architecture of a typical deployment. We then covered how to secure identities that access your environment using conditional access and how to collect audit logs. Proceeding this, we illustrated how to secure user data with FSLogix profiles and Disk Encryption. Securing the session hosts and applications, covering Azure Defender for Endpoint, AppLocker, Patching, lockdown, and managing Microsoft 365 security followed. Finally, we provided guidance on securing network access for Azure Virtual Desktop, covering topics such as Reverse Connect, Azure Firewall, and Azure Security Baseline.

We hope this handbook on Azure Virtual Desktop security fundamentals gave you a better understanding of how to keep your customers' Azure Virtual Desktop deployments secure! Check out the Resources section for additional reading and support to help you get started.

Resources

As you advance in your journey with Azure Virtual Desktop and enabling security, here are a few resources that can help:

- Read more about Azure Virtual Desktop Security best practices.
- Follow the Azure security baseline for Azure Virtual Desktop guidance.
- Test your Azure Virtual Desktop security knowledge with this learning module.
- Start now with an Azure free account.
- Contact Azure sales to get personalized guidance and discuss pricing, technical requirements, and solutions for enabling secure remote work.
- Join the Azure Migration and Modernization Program to get guidance and expert help in migrating your on-premises VDI.

Glossary

The following table contains a glossary of the terminology used throughout this handbook.

Term	Description
Active Directory Domain Services	A directory is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators.
Azure Active Directory (Azure AD)	Azure AD is Microsoft's cloud-based identity and access management service, which helps your employees sign in and access resources.
Microsoft Defender Application Control	Application Control was designed as a security feature under the servicing criteria defined by the Microsoft Security Response Center (MSRC) and allows you to control your Windows 10 devices with policies that define whether a specific driver or application can be executed on a device.
Microsoft Security Response Center (MSRC)	The Microsoft Security Response Center (MSRC) serves as Microsoft's single point of security coordination and communications and is led by some of the world's most experienced experts. The MSRC identifies, monitors, resolves, and responds to security incidents including vulnerabilities in Microsoft software.
FSLogix	FSLogix is designed to roam profiles in remote computing environments, such as Azure Virtual Desktop. It stores a complete user profile in a single container.
Azure Virtual Desktop	A desktop and app virtualization service that runs on Microsoft Azure.
Network security groups (NSGs)	An NSG contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.
AppLocker	AppLocker helps you control which apps and files users can run. These include executable files, scripts, Windows Installer files, dynamic-link libraries (DLLs), packaged apps, and packaged app installers.
Windows 10 Enterprise multi-session	Windows 10 Enterprise multi-session, formerly known as Windows 10 Enterprise for Virtual Desktops (EVD), is a new Remote Desktop session host that allows multiple concurrent interactive sessions.
Azure NetApp Files	The Azure NetApp Files service is an enterprise-class, high-performance, metered file storage service. Azure NetApp Files supports any workload type and is highly available by default.

About the author

Freek Berson is a Cloud Solutions Architect with a specialization in application and desktop delivery based on remoting technology. He has a long track record in the RDS space and has been awarded Microsoft Most Valuable Professional (MVP) since 2011.

Freek actively engages with the community. He speaks at various conferences around the world, including Microsoft Ignite, Microsoft Ignite | The Tour, Microsoft TechSummit, Microsoft TechDays, Azure Saturday, BriForum, E2EVC, ExpertsLive, and many more (online) events. He is also a published book author.

He works at Wortell, a cloud integrator company based in the Netherlands, where he focuses on end user computing, mostly on the Microsoft platform, with a strong focus on Azure.

He is also a managing partner at RDS Gurus. He maintains his personal blog at themicrosoftplatform.net, where he writes articles and blog posts related to Azure Virtual Desktop, RDS, Azure, and other Microsoft technologies.

You can follow him on Twitter at @fberson and check his contributions through his GitHub account.