aws

Administration Guide

Amazon WorkSpaces Core

Amazon WorkSpaces Core: Administration Guide

Table of Contents

Administration guides for partner solutions on Amazon WorkSpaces Core

Amazon WorkSpaces Core offers managed virtual desktop infrastructure designed to work with third-party management solutions. For more information, see Amazon WorkSpaces Core. Amazon WorkSpaces Core is part of the Amazon WorkSpaces Family of services. Amazon WorkSpaces Core gives technology partners like you flexibility and choice, while maintaining the security, global reliability, and cost efficiency customers have enjoyed from WorkSpaces for years. For more information, see Amazon WorkSpaces Family.

Amazon WorkSpaces Core supports two provisioning options:

- **Amazon WorkSpaces Core bundles** – Similar to an Amazon WorkSpaces Personal bundle, an Amazon WorkSpaces Core bundle is a preconfigured combination of compute, storage, and software resources, along with an operating system that you can use to launch a virtual desktop in Amazon WorkSpaces Core. Use this option to deliver persistent desktops where user data and settings are preserved. Amazon WorkSpaces Core manages the underlying infrastructure on your behalf, including Amazon Machine Image (AMI), Amazon EC2 instances, and Amazon EBS volumes. Pricing is all-inclusive and available on hourly or monthly billing terms. For details about available public bundles, see Deployment with WorkSpaces Core bundles.
- **Amazon WorkSpaces Core Managed Instances** – An Amazon WorkSpaces Core Managed Instance is an EC2 instance that is launched and managed by WorkSpaces Core. Use this option if you prefer to have more visibility and control of the types of EC2 instances managed by WorkSpaces Core. This option allows you to leverage EC2 pricing models, including Reserved Instances and Savings Plans, for cost optimization. You are billed for an hourly service fee in addition to charges for any AWS resources used (such as EC2 and EBS). For details about support instances, see Deployment with WorkSpaces Core Managed Instances.

WorkSpaces Core APIs require integration from VDI management solution partners. Workspot integrates with WorkSpaces Core Managed Instances while Citrix, Omnissa, and Leostream support WorkSpaces bundle configurations.

If you are an administrator who wants an immediate solution to configuring workspaces, without having to build or develop your own solution with Amazon WorkSpaces Core, please refer to the following administration guides from our partners:

- If you want to set up Citrix DaaS on Amazon WorkSpaces Core, see Citrix DaaS for Amazon WorkSpaces Core.
- If you want to set up Workspot Cloud PCs with Amazon WorkSpaces Core, see Getting Started with Workspot.
- If you want to set up Leostream with Amazon WorkSpaces Core, see Using Leostream to Manage Amazon WorkSpaces Core.
- If you want to set up Omnissa Horizon with Amazon WorkSpaces Core, see Deploying Omnissa Horizon 8 or Omnissa Horizon Cloud.

Using Amazon WorkSpaces Core Bundles

Similar to Amazon WorkSpaces personal bundles, a WorkSpaces Core bundle is a predefined combination of an operating system, compute, storage, and software resources. When launching a WorkSpaces, you select the bundle that best meets your requirements. The default bundles provided by WorkSpaces are referred to as public bundles. For more information, see Amazon WorkSpaces Bundles.

A custom image contains only the operating system, installed software, and user-defined settings for the WorkSpace. A custom bundle combines that custom image with the selected hardware specifications—such as compute and storage—that define the configuration of the WorkSpace.

After creating a custom image, you can build a custom bundle by selecting the appropriate compute and storage resources to pair with the image. This custom bundle can then be used to launch new WorkSpaces with a consistent configuration, ensuring standardization across your deployments.

To apply software updates or install additional applications, you can modify your custom bundle and use it to rebuild your WorkSpaces.

For a list of available WorkSpaces Core bundles, visit the Amazon WorkSpaces Core pricing page. To help you choose the right bundle for your use case, refer to the available bundle options.

Using Amazon WorkSpaces Managed Instances

An Amazon WorkSpaces Core Managed Instance is an EC2 instance that is launched and managed by WorkSpaces Core. If you choose to use WorkSpaces Core Managed Instances, you will manage your own AWS infrastructure and WorkSpaces Core is responsible for tasks such as provisioning

the instance, configuring software, scaling capacity, handling instance failures and replacements, and terminating the instance. You can deliver both persistent and non-persistent desktops while maintaining direct control over your EC2 instances launched through WorkSpaces Core. This option allows you to leverage EC2 pricing models, including Reserved Instances and Savings Plans, for cost optimization. You are billed for an hourly service fee in addition to charges for any AWS resources used (such as EC2 and EBS).

WorkSpaces Core Managed Instances only support instances with all sizes as shown below:

Purpose	Size
General purpose	M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6a | M6g | M6gd | M6i | M6id | M6idn | M6in | M7a | M7g | M7gd | M7i | M7i-flex | M8g | M8gd | T3 | T3a | T4g
Compute optimized	C5 | C5a | C5ad | C5d | C5n | C6a | C6g | C6gd | C6gn | C6i | C6id | C6in | C7a | C7g | C7gd | C7gn | C7i | C7i-flex | C8g | C8gd
Memory optimized	R5 | R5a | R5ad | R5b | R5d | R5dn | R5n | R6a | R6g | R6gd | R6i | R6idn | R6in | R6id | R7a | R7g | R7gd | R7i | R7iz | R8g | R8gd | X2gd | X2idn | X2iedn | X2iezn | X8g | z1d
Accelerated computing	G4ad | G4dn | G5 | G5g | G6 | G6e | Gr6 | P3dn | P4d | P4de | P5 | P5e | P5en

Note

Bare metal sizes such as m7i.metal-24xlarge are not supported.

For a list of available WorkSpaces Core bundles, visit the Amazon WorkSpaces Core pricing page. To help you choose the right instances for your use case, refer to Amazon EC2 instance types.

Security in Amazon WorkSpaces Core Managed Instances

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to WorkSpaces, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations

This documentation helps you understand how to apply the shared responsibility model when using WorkSpaces. It shows you how to configure WorkSpaces to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your WorkSpaces resources.

> **Note**
>
> Security for Amazon WorkSpaces Core Bundles is same as Amazon WorkSpaces. For more information on WorkSpaces Core Bundles security guidelines, please refer to Security in Amazon WorkSpaces in the *Amazon WorkSpaces Administration Guide*.

Contents

- Resilience in Amazon WorkSpaces Instances
- Infrastructure security in Amazon WorkSpaces Instances

Data protection in Amazon WorkSpaces Instances

The AWS shared responsibility model applies to data protection in Amazon WorkSpaces Core. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail. For information about using CloudTrail trails to capture AWS activities, see Working with CloudTrail trails in the *AWS CloudTrail User Guide*.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-3 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-3.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with Amazon WorkSpaces Core or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly

recommend that you do not include credentials information in the URL to validate your request to that server.

Encryption at rest

You can encrypt the storage volumes for your WorkSpaces Instances using AWS KMS Key from AWS Key Management Service. For more information, see Encryption at rest and Amazon EBS Encryption in the *Amazon EC2 User Guide*.

Encryption in transit

See Encryption in transit in the *Amazon EC2 User Guide*.

Identity and access management for WorkSpaces Instances

By default, IAM users don't have permissions for WorkSpaces Instances resources and operations. To allow IAM users to manage WorkSpaces resources Instances, you must create an IAM policy that explicitly grants them permissions, and attach the policy to the IAM users or groups that require those permissions.

To provide access, add permissions to your users, groups, or roles:

- Users and groups in AWS IAM Identity Center:

  Create a permission set. Follow the instructions in Create a permission set in the *AWS IAM Identity Center User Guide*.
- Users managed in IAM through an identity provider:

  Create a role for identity federation. Follow the instructions in Create a role for a third-party identity provider (federation) in the *IAM User Guide*.
- IAM users:
  - Create a role that your user can assume. Follow the instructions in Create a role for an IAM user in the *IAM User Guide*.
  - (Not recommended) Attach a policy directly to a user or add a user to a user group. Follow the instructions in Adding permissions to a user (console) in the *IAM User Guide*.

Following are additional resources for IAM:

- For more information about IAM policies, see Policies and Permissions in the *IAM User Guide* guide.
- For more information about IAM, see Identity and Access Management (IAM) and the *IAM User Guide*.
- For more information about WorkSpaces Instances specific resources, actions, and condition context keys for use in IAM permission policies, see Actions, Resources, and Condition Keys for Amazon WorkSpaces Managed Instances in the *IAM User Guide*.
- For a tool that helps you create IAM policies, see the AWS Policy Generator. You can also use the IAM Policy Simulator to test whether a policy would allow or deny a specific request to AWS.

Contents

Amazon WorkSpaces Instances example policies

The following example shows policy statements that you could use to grant access to perform WorkSpaces Instances tasks.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-instances:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus"
                "ec2:StopInstances",
                "ec2:StartInstances",
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DeleteVolume",
                "ec2:CreateVolume",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": "workspaces-instances.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

Note

In place of *, grant permissions to the specific KMS key that you are using.

If you are using the Amazon WorkSpaces Console, you will also need to add the following permissions:

```
iam:GetRole
iam:CreateServiceLinkedRole
```

> **Note**
>
> If you have already onboarded using Amazon WorkSpaces Console, `iam:CreateServiceLinkedRole` is optional.

Additional permissions may be required for specific partner requirements. For more information on partner permissions, refer to your partner specific guides.

Specify WorkSpaces resources in an IAM policy

To specify an WorkSpaces Instances resource in the `Resource` element of the policy statement, use the Amazon Resource Name (ARN) of the resource. You control access to your WorkSpaces Instances resources by either allowing or denying permissions to use the API actions that are specified in the `Action` element of your IAM policy statement. WorkSpaces Instances defines ARNs for WorkSpaces Instances, bundles, IP groups, and directories.

WorkSpaces Instances Instance ARN

A WorkSpaces Instances ARN has the syntax shown in the following example.

```
arn:aws:workspaces-instances:region:account_id:workspaceinstance/
workspace_instance_identifier
```

region

The Region that the WorkSpaces Instance is in (for example, `us-east-1`).

account_id

The ID of the AWS account, with no hyphens (for example, `123456789012`).

workspace_instance_identifier

The ID of the WorkSpaces Instance (for example, `"Resource": "arn:aws:workspaces-instances:region:account_id:workspaceinstance/workspace_instance_identifier"`).

You can use the * wildcard to specify all WorkSpaces Instances that belong to a specific account in a specific Region.

Using service-linked roles for Amazon WorkSpaces Instances

Amazon WorkSpaces Instances uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to WorkSpaces Instances. Service-linked roles are predefined by WorkSpaces Instances and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up WorkSpaces Instances easier because you don’t have to manually add the necessary permissions. WorkSpaces Instances defines the permissions of its service-linked roles, and unless defined otherwise, only WorkSpaces Instances can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting their related resources. This protects your WorkSpaces Instances resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have **Yes** in the **Service-linked roles** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for WorkSpaces Instances

WorkSpaces Instances uses the service-linked role named **AWSServiceRoleForWorkSpacesInstances** – This service linked role provides administrative access to Amazon WorkSpaces to manage EC2 instances in your AWS account.

The AWSServiceRoleForWorkSpacesInstances service-linked role trusts the following services to assume the role:

- `workspaces-instances.amazonaws.com`

It uses the following policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeVolumes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:TerminateInstances",
                "ec2:DeleteVolume",
                "ec2:StopInstances",
                "ec2:StartInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ec2:ManagedResourceOperator": "workspaces-instances.amazonaws.com"
                }
            }
        }
    ]
}
```

The role permissions policy named AWSServiceRolePolicyForWorkspacesInstances allows WorkSpaces Instances to complete the following actions on the specified resources:

- For monitoring your resources: `ec2:DescribeInstances`, `ec2:DescribeInstanceStatus`, and `ec2:DescribeVolumes`.
- For managing the ec2 instances which workspaces-instances.amazonaws.com operate: `ec2:TerminateInstances`, `ec2:DeleteVolume`, `ec2:StopInstances`, and `ec2:StartInstances`.

You must configure permissions to allow your users, groups, or roles to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the *IAM User Guide*.

Creating a service-linked role for WorkSpaces Instances

You can use either the IAM or WorkSpaces console to create a service-linked role with the **Workspaces instances** use case.

If you are using either the AWS CLI or the AWS API, create a service-linked role with the `workspaces-instances.amazonaws.com` service name.

For more information, see Creating a service-linked role in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

Editing a service-linked role for WorkSpaces Instances

WorkSpaces Instances does not allow you to edit the AWSServiceRoleForWorkSpacesInstances service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the *IAM User Guide*.

Deleting a service-linked role for WorkSpaces Instances

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

> **Note**
>
> If the WorkSpaces Instances service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To remove WorkSpaces Instances resources used by the AWSServiceRoleForWorkSpacesInstances

1. Use the ec2 console or api to list all the volumes with the operator.principal being workspaces-instances.amazonaws.com.
2. Delete all those volumes using the console or api of workspaces-instances service.
3. Delete all WorkSpaces instances in your account.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForWorkSpacesInstances service-linked role. For more information, see Deleting a service-linked role in the *IAM User Guide*.

Supported Regions for WorkSpaces Instances service-linked roles

WorkSpaces Instances supports using service-linked roles in all of the Regions where the service is available. For more information, see AWS Regions and endpoints.

Compliance validation for Amazon WorkSpaces Instances

Third-party auditors assess the security and compliance of Amazon WorkSpaces as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using WorkSpaces is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- Evaluating Resources with Rules in the *AWS Config Developer Guide* – AWS Config; assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Resilience in Amazon WorkSpaces Instances

The AWS global infrastructure is built around AWS Regions and Availability Zones. Regions provide multiple physically separated and isolated Availability Zones, which are connected through low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

Infrastructure security in Amazon WorkSpaces Instances

As a managed service, Amazon WorkSpaces Core is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see AWS Cloud Security. To design your AWS environment using the best practices for infrastructure security, see Infrastructure Protection in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access Amazon WorkSpaces Core through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

Refer to Infrastructure security in Amazon EC2.

Make Amazon WorkSpaces Instances API requests through a VPC interface endpoint

You can connect directly to Amazon WorkSpaces Instances API endpoints through an interface endpoint in your virtual private cloud (VPC) instead of connecting over the internet. When you

use a VPC interface endpoint, communication between your VPC and the Amazon WorkSpaces API endpoint is conducted entirely and securely within the AWS network.

The Amazon WorkSpaces Instances API endpoints support Amazon Virtual Private Cloud (Amazon VPC) interface endpoints that are powered by AWS PrivateLink. Each VPC endpoint is represented by one or more network interfaces (also known as elastic network interfaces, or ENIs) with private IP addresses in your VPC subnets.

The VPC interface endpoint connects your VPC directly to the Amazon WorkSpaces Instances API endpoint without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. The instances in your VPC don't need public IP addresses to communicate with the Amazon WorkSpaces Instances API endpoint.

You can create an interface endpoint to connect to Amazon WorkSpaces Instances with either the AWS Management Console or AWS Command Line Interface (AWS CLI) commands. For instructions, see Creating an Interface Endpoint.

After you have created a VPC endpoint, you can use the following example CLI commands that use the `endpoint-url` parameter to specify interface endpoints to the Amazon WorkSpaces Instances API endpoint:

```
aws workspaces-instances list-regions --region us-west-2 \
--endpoint https://workspaces-instances.us-west-2.api.aws
```

If you enable private DNS hostnames for your VPC endpoint, you don't need to specify the endpoint URL. The Amazon WorkSpaces Instances API DNS hostname that the CLI and Amazon WorkSpaces Instances SDK use by default (workspaces-instances.*externalRegion.api.aws*) resolves to your VPC endpoint.

The Amazon WorkSpaces Instances API endpoint supports VPC endpoints in all AWS Regions where both Amazon VPC and Amazon WorkSpaces Instances are available. Amazon WorkSpaces supports making calls to all of its public APIs inside your VPC.

To learn more about AWS PrivateLink, see the AWS PrivateLink documentation. For the price of VPC endpoints, see VPC Pricing. To learn more about VPC and endpoints, see Amazon VPC.

To see a list of Amazon WorkSpaces Instances API endpoints by Region, see WorkSpaces API Endpoints.

Note

Amazon WorkSpaces Instances API endpoints with AWS PrivateLink are not supported for Federal Information Processing Standard (FIPS) Amazon WorkSpaces Instances API endpoints.

Create a VPC endpoint policy for Amazon WorkSpaces Instances

You can create a policy for Amazon VPC endpoints for Amazon WorkSpaces Instances to specify the following:

- The principal that can perform actions.
- The actions that can be performed.
- The resources on which actions can be performed.

For more information, see Controlling Access to Services with VPC Endpoints in the *Amazon VPC User Guide*.

Note

VPC endpoint policies aren't supported for Federal Information Processing Standard (FIPS) Amazon WorkSpaces Instances endpoints.

The following example VPC endpoint policy specifies that all users who have access to the VPC interface endpoint are allowed to invoke the Amazon WorkSpaces hosted endpoint named `vpce-00b4e19feaf8b3eee` and VPC `vpc-0ecfe75f77ce1aa61`.

```
{
    "Statement": [
        {
            "Action": "workspaces-instances:ListRegions",
            "Condition": {
                "StringEquals": {
                    "aws:SourceVpc": "vpc-0ecfe75f77ce1aa61",
                    "aws:SourceVpce": "vpce-00b4e19feaf8b3eee"
                }
```

```
            },
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Resource": "*",
            "Sid": "AllowPortalsAccess"
        }
    ],
    "Version": "2012-10-17"
}
```

> **Note**
>
> In this example, users can still take other Amazon WorkSpaces Instances API actions from outside the VPC. To restrict API calls to those from within the VPC, see Identity and access management for WorkSpaces Instances for information about using identity-based policies to control access to Amazon WorkSpaces Instances API endpoints.

Connect your private network to your VPC

To call the Amazon WorkSpaces Instances API through your VPC, you have to connect from an instance that is inside the VPC, or connect your private network to your VPC by using AWS Virtual Private Network (AWS VPN) or AWS Direct Connect. For information, see VPN Connections in the *Amazon Virtual Private Cloud User Guide*. For information about AWS Direct Connect, see Creating a Connection in the *AWS Direct Connect User Guide*.

Document history for the Amazon WorkSpaces Core Administration Guide

The following table describes the documentation releases for Amazon WorkSpaces Core.

Change	Description	Date
Added new topic	Added Security section	June 23, 2025
New and updated link	Added link to Citrix Daas and updated Workspot link	April 1, 2024
Initial release	Initial release of the Amazon WorkSpaces Core Administration Guide	September 20, 2023