Quest® On Demand

Policy Management for Skype for Business Online User Guide

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

On Demand Policy Management for Skype for Business Online User Guide
Updated - July 2017

Contents

1

Policy Management for Skype for Business Online User Guide

The Policy Management for Skype for Business Online User Guide covers the following topics:

- Documentation roadmap
- Introduction to Quest On Demand
- Policy Managment
- Glossary

2

Documentation roadmap

Global settings

On Demand global settings refers to management tools and configuration settings that apply to all On Demand modules. This includes tenant management tasks and downloading audit logs.

Modules

Each management tool is referred to as a module. Currently, the following modules are available:

- Policy Management for Skype for Business Online
- Policy Management for Exchange Online
- Recovery for Azure Active Directory

Documentation

For each module, and the global settings, there is a Release Notes document and a User Guide.

- The Release Notes contains a release history and details of new features, resolved issues, and known issues.
- User Guides contain descriptions and procedures for the management tasks you can perform with each module.

Use the links below to navigate to the content you require.

User Guides

- Global Settings
- Policy Management for Skype for Business Online
- Policy Management for Exchange Online
- Recovery for Azure Active Directory

Release Notes

- Global Settings
- Policy Management for Skype for Business Online
- Policy Management for Exchange Online
- Recovery for Azure Active Directory

More Resources

- For sales or other inquiries, visit http://quest.com/company/contact-us.aspx or call +1-949-754-8000.
- To sign up for a trial or purchase a subscription, go to https://www.quest.com/on-demand.
- Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.
- The Quest On Demand Community provides a space for blog posts and a forum to disucss the On Demand products.

3

Introduction to Quest On Demand

- Overview
- Modules
- Organizations
- Azure Active Directory tenants

Overview

On Demand is a cloud based management platform, providing access to multiple Quest Software Microsoft management tools through a single interface. Cloud based is a term that refers to applications, services or resources made available to users on demand via the Internet. Quest On Demand is a Software as a Service (SaaS) application where application software is hosted in the cloud and made available to users through quest-on-demand.com.

On Demand management is based on the concepts of organizations, modules, and Azure Active Directory (AD) tenants. When you sign up for the On Demand service, you create an organization. The organization can subscribe to modules. Organization administrators can use the tools provided by the modules to perform administrative actions on Azure AD tenants.

Modules

Each management tool is referred to as a module. Currently, the following modules are available:

- Policy Management for Skype for Business Online
- Policy Management for Exchange Online
- Recovery for Azure Active Directory

Global settings

On Demand Global Settings refers to management tools and configuration settings that apply to all On Demand modules. This includes tenant management tasks and downloading audit logs.

Organizations

On Demand administration is based on organizations. When a user signs up for On Demand, an organization is created.

You can add users to an organization. To add a user, click **Settings** in the navigation panel on the left and then click **Permissions**.

Azure Active Directory tenants

Microsoft Azure also uses the concept of an organization. An Azure Active Directory (Azure AD) tenant is representative of an organization. It is a dedicated instance of the Azure AD service that an organization receives and owns when it signs up for a Microsoft cloud service such as Azure, Microsoft Intune, or Office 365. Each Azure AD tenant is distinct and separate from other Azure AD tenants.

A tenant houses the users in a company and the information about them - their passwords, user profile data, permissions, and so on. It also contains groups, applications, and other information pertaining to an organization and its security. For more information see this Microsoft help page.

•

4

Policy Managment

There are many Skype for Business Online policies and each policy can have many settings. Typically, policy settings must be managed using a PowerShell cmdlet. With the On Demand for Skype for Business Online module, you can manage policies through an intuitive user interface. Policies can be applied in bulk to target users and groups and the module automatically detects group changes. The application of policies can be scheduled in order to maintain the correct Skype for Business Online settings across the organization.

To manage Skype for Business Online policies, perform the following tasks:

- Selecting a tenant
- Applying policies

Selecting a tenant

Before proceeding to the Policy Management for Skype for Business Online main page, you must select a tenant.

- Viewing available tenants
- Tenant policy rule status indicators
- Required tenant credentials
- Selecting a tenant

Viewing available tenants

Policy management actions are applied to a single tenant. The Policy Management for Skype for Business Online tenant page displays a list of tenants that have been added to an organization.

To add a tenant, select **Tenants** in the side navigation panel. For more information, click the help icon on the **Tenant** page or see Tenant Management in the *On Demand Global Settings User Guide*.

! **CAUTION: Adding a tenant to multiple organizations**

Adding the same tenant to multiple organizations can result in conflicting application of polices and settings. When using multiple organizations to manage a tenant, the organization administrators must coordinate their management activities.

Tenant policy rule status indicators

For each tenant, the following rule status indicators are displayed.

Table 1. Tenant rule status

	**In Progress** When policy settings are being applied based on currently enabled rules, the numeric value indicates per cent completed.

Table 1. Tenant rule status

	Completed Application of policy settings is complete.
	Error When policy settings are being applied based on currently enabled rules, the numeric value indicates the number of errors. You can view the list of errors for each individual policy rule. On the Policy Management page, select a rule and then click the **Error** icon for the rule.

Required tenant credentials

> **IMPORTANT:** Quest recommends that you create a dedicated Office 365 account to manage Skype for Business Online policies using On Demand.
>
> If the account is not dedicated, conflicts may cause the account to become locked out from the On Demand application.

Skype for Business Online is part of the Office 365 suite of services. In order to perform policy management on a tenant, you must enter your Office 365 credentials for the tenant. Providing your administrator credentials establishes a remote connection to the required PowerShell cmdlets for the module.

The following Office 365 administrator roles grant full access to Skype for Business Online:

- Global administrator
- User management administrator
- Password administrator
- Skype for Business administrator

Selecting a tenant

Prerequisites

Before selecting a tenant on which to perform policy management, you must:

- have already added a tenant to your On Demand organization
- be able to log in with Office 365 administrator credentials

To select a tenant for policy management:

1. Log in to On Demand.
2. Select the Policy Management module.

   On Demand displays all the tenants that have been added to your organization. If Office 365 administrator credentials have not been entered, the tenant shows **Add Credentials**.
3. If required, click **Add Credentials**.
4. Enter the user name a password for an Office 365 administrator.
5. Click **Select**.

   The User Policy Rules page opens.

Applying policies

- Creating policy rules
- Enabling and applying policy rules

Creating policy rules

To manage Skype for Business Online policies you must define policy rules. You can define multiple rules and apply them. On Demand applies the rules sequentially based on the ordering in the **Rules** list.

A rule defines one or more Skype for Business Online policy settings and identifies one or more target users for the policy.

- Global policy rule status indicators
- Settings
- Target Users and Groups
- Policies to Apply
- Adding and Editing rules

Global policy rule status indicators

There are two levels of rule status reporting: global and per selected rule.

The global status indicators are located above the **Settings** panel and provide information for all enabled rules.

Table 2. Global policy rule status

	**In Progress** When policy settings are being applied based on currently enabled rules, the numeric value indicates per cent completed.
	**Completed** Application of policy settings is complete.
	**Users** When policy settings are being applied based on currently enabled rules, the numeric value indicates the number of users whose policy settings will be updated. Note that an unusual user number could indicate that a higher rule has blocked the application of a policy in a lower rule
	**Error** When policy settings are being applied based on currently enabled rules, the numeric value indicates the number of errors. You can view the list of errors for each individual policy rule. Select a rule and then click the **Error** icon for the rule.

Settings

The **Enabled** check box is grayed out until you add a target user or group to a rule and specify a policy setting. Once the **Enabled** box is checked and the rule is saved, the rule policy settings are applied. For more information, see Enabling and applying policy rules on page 14.

Individual policy rule status indicators

The status indicators in the Settings panel provide status information for the currently selected rule.

Table 3. Selected rule status

	**Progress** For the currently selected rule, the numeric value indicates per cent completed.
	**Completed** Application of policy settings is complete.
	**Users** For the currently selected rule, the numeric value indicates the number of users whose policy settings will be updated.
	**Error** For the currently selected rule, the numeric value indicates the number of errors. To view the errors, click the icon to view the Errors list.

Target Users and Groups

On Demand polices are applied to Office 365 users and groups. Once you define an On Demand policy rule for a user or group, those users become On Demand managed users.

Office 365 users and groups

In the On Demand Skype for Business Online Policy Management module, **Target Users and Groups** are Office 365 users that have been enabled for Skype for Business Online in the currently selected tenant. Once you start typing in the **Target Users and Groups** field, On Demand automatically completes the entry based on the current user list.

Users can be added individually or in bulk using the Office 365 Admin Center. You can also replicated Active Directory accounts in Office 365. For more information, see this Microsoft help page.

Groups can be created in a number of ways. For example, you can create groups in the Office 365 Admin Center. For more information see this Microsoft help page. Organizing users into groups allows you to refine the application of policies to suit the needs of your organization.

Managed users

An On Demand managed user is a target for one or more policy rules. To ensure all users in your organization are managed, create global policy rules that set company default policies for all users. Place global rules at the bottom of the **Rules List**. Refine your policy settings by creating additional policy rules for specific users and placing them above the global rules in the rules list. See Rule order and policy precedence on page 14.

> **IMPORTANT: Deleting Rules**
>
> When you delete a rule, users can become unmanaged. Policy settings remain as currently configured.
>
> - If a rule has already been applied, the applied settings do not revert back when a rule is deleted.
> - If you delete an enabled rule and provisioning is in progress, then provisioning is stopped. Policies already applied remain in place and do not revert back.

Policies to Apply

On Demand manages Skype for Business Online policy settings for user accounts in a specific tenant. Policies determine the Skype for Business Online capabilities that are available to users and to the organization as a whole.

In practice, the five most commonly used policies are:

- **Client:** Determines the features of Skype for Business that are available to users. For example, presence states or the ability to transfer files.
- **Conferencing:** Determines the features and capabilities that can be used in a conference. You can use conferencing policies to manage security, bandwidth, and legal aspects of meetings such as recording.
- **Voice:** Determines the availability of Enterprise voice features such as call forwarding.
- **External Access:** Determines if users can communicate with users outside of the organization.
- **Mobility:** Determines the features and capabilities that can be used on mobile devices.

When Skype for Business Online licenses are applied to new users, Skype for Business Online assigns global policies or plan specific initial policies to the new users.The Skype for Business Online environment can be fine-tuned by applying specific policies to users and groups. The per-user policy scope is also referred to as the tag scope. Per-user policies take priority over global policies.

Policy setting details and Microsoft help

- `Get` cmdlet: You can run PowerShell `Get` cmdlets against your tenant to determine what policies exist in the tenanat. These are the values displayed in the **Policies to Apply** drop down lists. The `Get` cmdlet also returns the current setting.
- `Set` cmdlet: For Microsoft documentation on the function of each policy setting, see the help pages for the `Set` cmdlet.
- Microsoft also provides help pages for planning policy settings.

Table 4. Microsoft help pages

Get cmdlet	Set cmdlet	Planning
Get-CsClientPolicy	Set-CsClientPolicy	Client
Get-CsConferencingPolicy	Set-CsConferencingPolicy	Conferencing
Get-CsVoicePolicy	Set-CsVoicePolicy	Voice
Get-CsExternalAccessPolicy	Set-CsExternalAccessPolicy	External Access
Get-CsMobilityPolicy	Set-CsMobilityPolicy	Mobility

Adding and Editing rules

To add a rule:

1. On the User Policy Rules page, click **Add rule**.
2. In the rule **Settings** panel, enter a **Rule Name**.
3. In the Target User or Groups field, type the name of a user or group.

   The field is automatically populated based on the users and groups in the tenant.
4. Click **Add**.

   The user or group is added to the target list.
5. Using the drop down policy lists, select the policies you want to apply.
6. Click **Save**.

   The rule is added to the **Rules** list.

NOTE: If you have enabled rules, clicking **Save** applies all enabled rules.

To edit a rule:

1. Select a rule in the **Rules** list.

2 Modify the rule **Settings** as required.

3 Click **Save**.

NOTE: If you have enabled rules, clicking **Save** applies all enabled rules.

Enabling and applying policy rules

- Rules list
- Rule order and policy precedence
- Applying a single rule
- Applying multiple rules
- Deleting a rule
- Verifying the application of a policy

Rules list

As you create rules, they are added to the **Rules** list. Click **Add rule** to add a rule to the list.

The rule status indicator are displayed to the right of the rule name.

Table 5. Rules list status indicators

	Disabled The rule is currently disabled. Click **Enabled** in the Settings panel to enable the rule.
	In Progress The rule is running and policies are being applied to the target users.
	Completed Application of policy settings is complete.
3	**Errors** The numeric value indicates the number of errors.

Rule order and policy precedence

Rules in the **Enabled** state are applied in order from top to bottom. When you enable and apply multiple rules:

- A rule higher in the list takes precedence over lower rules.
- Order the rules list from granular to global.

For example, if one user in a group requires a unique policy setting, the rule for the user must be higher in the list than the rule applying a different setting for the group. The policy setting for the group does not overwrite the user setting even though it is applied subsequently.

NOTE: NoChange setting.

For each rule, the default policy setting **NoChage** has no influence on subsequent rules. Policy changes in rules lower in the **Rules** list are applied even if a higher rule is applied with the **NoChange** setting for the policy.

To reorder the **Rules** list, click on the bar to the left of the rule number and drag it to a new ordered position.

Rule ordering best practices

Rules must be ordered from granular to global. Below are two possible methods of ordering your rules.

Method 1. Each rule applies the same set of policy types and rules are ordered by target group:

1. John Smith
2. Toronto
3. Boston
4. Canada
5. U.S.
6. Worldwide

Method 2. Each rule applies a specific policy type and rules are ordered by target group:

1. Conferencing - John Smith
2. Conferencing - Toronto
3. Conferencing- Boston
4. Conferencing - Canada
5. Conferencing - US
6. Conferencing - Worldwide
7. Client - Jane Doe
8. Client - Development
9. Client - Sales
10. Client - Worldwide

Hierarchical rule order example

John Smith is a member of the Business Unit group and he requires the ability to save and archive instant message sessions. The remainder of the Business Unit group will not have access to this feature. To apply these policies create the following rules in order.

Table 6.

Rules	Target User or Group	Policies to Apply - Client
Rule 1	John Smith	NoChange
Rule 2	Business Unit group	ClientPolicyNoSaveIMNoArchiving

Applying a single rule

Once you have defined a rule, you can apply the new policy settings to the tenant.

Once you have defined the **Target Users or Groups** and the **Policies to Apply**, you can apply a rule immediately by selecting the **Enable** check box and clicking **Save**.

To apply a single rule from the **Rules** list, enable only that rule and click **Save**.

Applying multiple rules

If you have defined multiple rules, you can determine which rules to apply by enabling or disabling rules in the **Rules** list. Each time you click **Save** the provisioning process is restarted and all enabled rules are applied in order.

Reordering rules in the **Rules** list also restarts the provisioning process and applies all enabled rules in order. To reorder the **Rules** list, click on the bar to the left of the rule number and drag it to a new ordered position.

NOTE: Changing the **Rule Name** and clicking **Save** does not restart the provisioning process.

Deleting a rule

When you delete a rule, policy settings remain as currently configured. If a rule has already been applied, the applied settings do not revert back when a rule is deleted.

If you delete an enabled rule and provisioning is in progress, then provisioning is stopped. Policies already applied remain in place.

To delete a rule, select the rule in the **Rules** list and click **Delete**.

Verifying the application of a policy

To verify that a policy has been applied, use the following PowerShell cmdlet:

```
Get-CsOnlineUser [-Identity <UserIdParameter>]
```

For more information, see this Microsoft help page.

5

Glossary

Administrator roles

Microsoft Azure AD Global Administrator	The Microsoft Azure AD Global administrator is the top level administrator role and has access to all features. The person who signs up for Azure becomes the Global Administrator.
Office 365 Global Administrator	The Office 365 Global administrator has access to all Skype for Business Online administrative features.
On Demand Organization Administrator	The On Demand organization administrator role is the top level administrator role and has access to all features. By default, the user that completes the On Demand **Sign Up** process is assigned to the On Demand organization administrator role for the organization.
Module Administrator	Module administrators have permission to perform task in specific modules. You can add multiple module administrators to your On Demand organization

Admin consent

The process of approving the use of an application for the whole Microsoft Azure AD organization by the Microsoft Global administrator is referred to as admin consent. The Microsoft Global administrator must provide admin consent when adding a tenant to On Demand.

When a tenant is first added, On Demand requests base admin consent permissions. Some modules can function using the base permission set while other require a higher level of admin consent permissions.

On Demand organization

On Demand administration is based on organizations. When a user signs up for On Demand, an organization is created. Administrators perform management tasks on Microsoft Active Directory tenants that have been added to the organization. A user may belong to only one organization.

Microsoft organizational account

When you subscribe to Microsoft Azure, you create an organizational account. The subscription process prompts you to provide details about your organization and your organization’s internet domain name registration. The organization information is used to create a new Azure Active Directory instance for the organization.

Microsoft documentation sometimes refers to **Organizational Accounts** as **Work or school Accounts** to distinguish them from **Microsoft Accounts**.

Microsoft Azure

A cloud computing service created by Microsoft. It is used by developers and IT professionals for building, deploying, and managing applications and services through a global network of Microsoft-managed data centers. Quest On Demand is hosted in Microsoft Azure.

Microsoft Azure Active Directory

Azure Active Directory (AD) is a multi-tenant, cloud based, directory and identity management service. For more information, see this Microsoft help page.

Tenant

In Azure Active Directory (Azure AD), a tenant is representative of a Microsoft Azure AD organization. It is a dedicated instance of the Azure AD service that an organization receives and owns when it signs up for a Microsoft cloud service such as Azure, Microsoft Intune, or Office 365. Each Azure AD tenant is distinct and separate from other Azure AD tenants.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit http://quest.com/company/contact-us.aspx or call +1-949-754-8000.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.

Index