One Identity Active Roles 7.2

Skype for Business Server User Management Administrator Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

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

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

Active Roles Skype for Business Server User Management Administrator Guide
Updated - December 2017
Version - 7.2

Contents

1

Solution Overview

Introducing Skype for Business Server User Management

The Skype for Business Server User Management solution enables Active Roles to administer Skype for Business Server user accounts. This solution provides built-in policies that synchronize user account information between Active Roles and Skype for Business Server, allowing Skype for Business Server user management tasks to be performed using Active Roles Web Interface.

With Skype for Business Server User Management, you can use Active Roles to perform the following tasks:

- Add and enable new Skype for Business Server users
- View or change Skype for Business Server user properties and policy assignments
- Move Skype for Business Server users from one Skype for Business Server pool to another
- Disable or re-enable user accounts for Skype for Business Server
- Remove users from Skype for Business Server

Skype for Business Server User Management adds the following elements to Active Roles:

- Built-in Policy Object containing a policy that enables Active Roles to perform user management tasks on Skype for Business Server.

- Built-in Policy Object containing a supplementary policy that enables Active Roles to administer Skype for Business Server usersin environments that involve multiple Active Directory forests.
- Commands and pages for managing Skype for Business Server users in the Active Roles Web Interface.
- Access Templates to delegate Skype for Business Server user management tasks.

The Skype for Business Server User Management policy allows you to control the following factors of Skype for Business Server user creation and administration:

- Rule for generating the SIP user name. When adding and enabling a new Skype for Business Server user, Active Roles can generate a SIP user name based on other properties of the user account.
- Rule for selecting a SIP domain. When configuring the SIP address for a Skype for Business Server user, Active Roles can restrict the list of selectable SIP domains and suggest which SIP domain to select by default.
- Rule for selecting a Telephony option. When configuring Telephony for a Skype for Business Server user, Active Roles can restrict the list of selectable Telephony options and suggest which option to select by default.
- Rule for selecting a Skype for Business Server pool. When adding and enabling a new Skype for Business Server user, Active Roles can restrict the list of selectable registrar pools and suggest which pool to select by default. This rule also applies to selection of the destination pool when moving a Skype for Business Server user from one pool to another.

Skype for Business Server User Management provides a number of Access Templates allowing you to delegate the following tasks in Active Roles :

- Add and enable new Skype for Business Server users
- View existing Skype for Business Server users
- View or change the SIP address for Skype for Business Server users
- View or change the Telephony option and related settings for Skype for Business Server users
- View or change Skype for Business Server user policy assignments
- Disable or re-enable user accounts for Skype for Business Server
- Move users from one Skype for Business Server pool to another
- Remove users from Skype for Business Server

Supported Active Directory topologies

Skype for Business Server User Management supports the same Active Directory Domain Services (AD DS) topologies as Microsoft Lync 2013 and Microsoft Lync 2010. The following topologies are supported:

- Single forest with a single tree or multiple trees
- Multiple forests in a resource forest topology
- Multiple forests in a central forest topology

Single forest

The single forest topology assumes that the logon-enabled user accounts managed by Active Roles are defined in the Active Directory forest in which Skype for Business Server is deployed. To perform Skype for Business Server user management tasks on a given user account, Active Roles makes changes to the attributes of that use account, and then, based on the attribute changes, the Skype for Business Server User Management policy requests the Skype for Business Server remote shell to update the user account accordingly. For example, when creating a new Skype for Business Server user, Active Roles sets a virtual attribute on that user's account directing the policy to invoke the remote shell command for enabling the new user for Skype for Business Server. When making changes to an existing Skype for Business Server user, Active Roles populates the attributes of the user's account with the desired changes, causing the policy to apply those changes via the remote shell.

Multiple forests - Resource forest

The resource forest topology refers to a multi-forest environment where a separate forest—Skype for Business Server forest—hosts servers running Skype for Business Server but does not host any logon-enabled user accounts. Outside the Skype for Business Server forest, user forests host logon-enabled user accounts but no servers running Skype for Business Server. When creating a Skype for Business Server account for a user from an external forest, Active Roles creates a disabled user account in the Skype for Business Server forest, establishes a link between the user account in the user forest (master account) and the disabled user account in the Skype for Business Server forest (shadow account), and enables the shadow account for Skype for Business Server. The Master Account Management policy then ensures that the attributes of the shadow account are synchronized with the attributes of the master account, so that Skype for Business Server user properties can be administered on the master account via Active Roles. In the Skype for Business Server forest, the User Management policy detects the attribute changes replicated from the master account to the shadow account, and translates them to remote shell commands on Skype for Business Server, similarly to the Single forest case.

Multiple forests - Central forest

The central forest topology refers to a multi-forest environment where a separate forest—Skype for Business Server forest—hosts servers running Skype for Business Server and may also host logon-enabled accounts. Outside the Skype for Business Server forest, user

forests host logon-enabled user accounts but no servers running Skype for Business Server.

With the Skype for Business Server User Management policy applied to logon-enabled user accounts in the Skype for Business Server forest, Active Roles can enable and administer those user accounts for Skype for Business Server in the same way as in the Single forest case.

When creating a Skype for Business Server account for a user from an external forest, Active Roles creates a contact in the Skype for Business Server forest, establishes a link between the user account in the user forest (master account) and the contact in the Skype for Business Server forest (shadow account), and enables that contact for Skype for Business Server. The Master Account Management policy then ensures that the attributes of the contact are synchronized with the attributes of the user account, so that Skype for Business Server user properties can be administered on the user account via Active Roles. In the Skype for Business Server forest, the User Management policy detects the attribute changes replicated from the user account to the contact, and translates them to remote shell commands on Skype for Business Server, similarly to the Single forest case.

User Management policy

The User Management policy is intended for single-forest and multi-forest environments where logon-enabled accounts of Skype for Business Server users are defined in the Active Directory forest in which Skype for Business Server is deployed, as well as for multi-forest environments where logon-enabled master accounts of Skype for Business Server users are defined in external forests with each master account being represented by a shadow account (disabled user account or contact) in the Active Directory forest in which Skype for Business Server is deployed. The User Management policy enables Active Roles to perform user management tasks on Skype for Business Server.

The Policy Object that holds this policy is in the **Configuration/Policies/Administration/Builtin** container. The name of the Policy Object is **Built-in Policy - Skype for Business - User Management**. Depending upon your Active Directory topology, apply this Policy Object as follows to enable Skype for Business Server User Management in Active Roles.

Table 1: Applying the Built-in - Skype for Business - User Management Policy Object

Topology option	Where to apply the Policy Object
Single forest	Apply this Policy Object to Active Directory domains or containers that hold user accounts you want to administer by using Skype for Business Server User Management in Active Roles.
Multiple forests	Apply this Policy Object to

Topology option	Where to apply the Policy Object
- Resource forest	Active Directory domains or containers in the Skype for Business Server forest that hold shadow accounts (disabled user accounts) for users from external forests you want to administer by using Skype for Business Server User Management in Active Roles.
Multiple forests - Central forest	Apply this Policy Object to Active Directory domains or containers in the Skype for Business Server forest that hold logon-enabled user accounts you want to administer by using Skype for Business Server User Management in Active Roles Active Directory domains or containers in the Skype for Business Server forest that hold shadow accounts (contacts) for users from external forests you want to administer by using Skype for Business Server User Management in Active Roles.

User Management policy settings

The topics in this section cover the User Management policy settings.

Connection to Skype for Business Server

To administer Skype for Business Server users, Active Roles requires a connection to a computer running the following server role in your Skype for Business Server deployment: Front End Server (in case of Skype for Business Server Enterprise Edition) or Standard Edition Server. The computer must be from an Active Directory domain that is registered with Active Roles as a managed domain. By using the **Server** policy setting, you can specify how you want Active Roles to select a Skype for Business Server computer:

- **Connect to any available server** With this option, Active Roles attempts to connect to any Front End Server or Standard Edition Server that runs the Central Management Server in your Skype for Business Server deployment. If no Central Management Server role holders are available in the managed domains, then Active Roles attempts to connect to the first Front End Server or Standard Edition Server found in the managed domains.
- **Connect to these servers only** This option allows you to configure a list from which you want Active Roles to select a Skype for Business Server computer. You can:
    - Add or remove computers from the list. Active Roles searches the managed domains for computers running the appropriate Skype for Business Server role, allowing you to select the desired computers.

- Set the default computer. Active Roles first attempts to connect to that computer.
- Reorder the list. Active Roles first attempts to connect to computers that are higher in the list.

Note that at least one of your Active Directory domains that hold computers running the Front End Server or Standard Edition Server must be registered with Active Roles as a managed domain. Otherwise, Active Roles is unable to discover your Skype for Business Server deployment, so Skype for Business Server User Management functions are unavailable.

SIP user name generation rule

The **SIP User Name** policy setting allows you to configure a rule for generating the SIP user name based on other properties of the user account. When adding a new Skype for Business Server user, Active Roles uses that rule to generate the SIP user name on the Web Interface page for enabling users for Skype for Business Server. The rule has an effect if you select the SIP address option that provides for entering a SIP user name. On the page where you edit Skype for Business Server users, the rule performs a validation function, preventing changes to the SIP user name that violate the rule.

To configure a rule, you set up a value that acts as a template for the SIP user name. You can add one or more entries to the value, with each entry representing one of the following:

- **Text** A text string. You can type the desired text when adding the entry.
- **User Property** A particular property of the user account. You can choose the desired property and specify whether you want the entry to include the entire property or a part of the property.
- **Parent OU Property** A particular property of the Organizational Unit that holds the user account. You can choose the desired property and specify whether you want the entry to include the entire property or a part of the property.
- **Parent Domain Property** A particular property of the Active Directory domain that holds the user account. You can choose the desired property and specify whether you want the entry to include the entire property or a part of the property.

The rule sets the SIP user name to the string value obtained by calculating each entry and then concatenating the calculation results so that they form a single string value.

By default, the policy allows the generated name to be modified. The **SIP User Name** policy setting provides the option to prevent changing the generated name. If you select that option, the SIP user name is read-only on the Web Interface page for enabling users for Skype for Business Server.

SIP domain restriction rule

The **SIP Domain** policy setting allows you to configure a rule that restricts selection of a SIP domain for the user SIP address. When you add a new Skype for Business Server user or edit an existing Skype for Business Server user, this rule determines the list from which you can select a SIP domain for the user's SIP address. In case of adding a new Skype for Business Server user, the rule applies to any SIP address option that involves selecting a SIP domain from the list.

To configure a rule, you choose one of these policy options:

- **Allow selection of any SIP domain** With this option, the policy does not restrict the list of SIP domains.
- **Restrict selection to these SIP domains** This option allows you to configure a list of acceptable SIP domains. You can:
  - Add or remove SIP domains from the list. Active Roles identifies all SIP domains that exist in your Skype for Business Server deployment, allowing you to select the desired SIP domains.
  - Set the default SIP domain. When creating a SIP address, Active Roles selects the specified SIP domain by default.
  - Reorder the list. When prompting to select a SIP domain for a user's SIP address, Active Roles lists the SIP domain names in the order specified.

Pool restriction rule

The **Pool** policy setting allows you to configure a rule that restricts selection of an Enterprise Edition Front End pool or Standard Edition server to which Skype for Business Server users can be assigned. When you add a new Skype for Business Server user, this rule determines the list from which you can select a pool for the new user. When you move a Skype for Business Server user from one pool to another, this rule determines the list from which you can select the destination pool.

To configure a rule, you choose one of these policy options:

- **Allow selection of any pool** With this option, the policy does not restrict the list of pools.
- **Restrict selection to these pool** This option allows you to configure a list of acceptable pools. You can:
  - Add or remove pools from the list. Active Roles identifies all Front End pools and Standard Edition servers in your Skype for Business Server deployment, allowing you to select the desired pools or servers.
  - Set the default pool. When adding a new Skype for Business Server user or moving a user to another pool, Active Roles selects the specified pool by default.
  - Reorder the list. When prompting to select a pool, Active Roles lists the pools in the order specified.

Telephony restriction rule

The **Telephony** policy setting allows you to configure a rule that restricts selection of a Telephony option for Skype for Business Server users. When you add or edit a Skype for Business Server user, this rule determines the list from which you can select a Telephony option.

To configure a rule, you choose one of these policy options:

- **Allow selection of any option** With this option, the policy does not restrict the list of Telephony options.
- **Restrict selection to these options** This option allows you to configure a list of acceptable Telephony options. You can:
  - Add or remove Telephony options from the list.
  - Set the default Telephony option. When adding a new Skype for Business Server, Active Roles selects the specified Telephony option by default.
  - Reorder the list. When prompting to select a Telephony option, Active Roles lists the options in the order specified.

Master Account Management policy

The Master Account Management policy is intended for multi-forest environments where logon-enabled master accounts of Skype for Business Server users are defined in Active Directory forests in which Skype for Business Server isn't deployed, with each master account being represented by a shadow account (disabled user account or contact) in the Active Directory forest in which Skype for Business Server is deployed (see Multiple forests - Resource forest and Multiple forests - Central forest earlier in this document). The Master Account Management policy enables Active Roles to control master accounts of Skype for Business Server users, and operates in conjunction with the User Management policy that controls shadow accounts in the Skype for Business Server forest.

The Policy Object that holds this policy is in the **Configuration/Policies/Administration/Builtin** container. The name of the Policy Object is **Built-in Policy - Skype for Business - Master Account Management**. Depending upon your Active Directory topology, apply this Policy Object as follows to enable Skype for Business Server User Management in Active Roles.

Table 2: Applying the Built-in - Skype for Business - Master Account Management Policy Object

Topology option	How to apply the Policy Object
Single forest	Do not apply this Policy Object
Multiple forests	Configure the **Forest Mode** policy setting by selecting the **Resource**

Topology option	How to apply the Policy Object
- Resource forest	**forest** option, and then apply this Policy Object to Active Directory domains or containers that hold logon-enabled user accounts in external forests (master accounts) you want to administer by using Skype for Business Server User Management in Active Roles.
Multiple forests - Central forest	Configure the **Forest Mode** policy setting by selecting the **Central forest** option, and then apply this Policy Object to Active Directory domains or containers that hold logon-enabled user accounts in external forests (master accounts) you want to administer by using Skype for Business Server User Management in Active Roles.

Master Account Management policy settings

The topics in this section cover the Master Account Management policy settings.

Skype for Business Server forest mode

The Master Account Management policy is intended for multi-forest environments where the Skype for Business Server forest is used either as a resource forest or as a central forest. In the central forest mode, the Skype for Business Server forest may hold logon-enabled Skype for Business Server user accounts in addition to shadow accounts (contacts) for Skype for Business Server users from external forests. In the resource forest mode, the Skype for Business Server forest holds only shadow accounts (logon-disabled user accounts) for Skype for Business Server users from external forests. The **Forest Mode** policy setting allows you to choose the option that matches the Skype for Business Server forest mode in your Skype for Business Server deployment:

- **Resource forest** The policy creates and administers logon-disabled user accounts as shadow accounts for Skype for Business Server users from external forests. The user account from an external forest, referred to as a master account, is linked and synchronized with the shadow account that is enabled for Skype for Business Server in the Skype for Business Server forest.
- **Central forest** The policy creates and administers contact objects as shadow accounts for Skype for Business Server users from external forests. The user account from an external forest, referred to as a master account, is linked and synchronizes with the contact that is enabled for Skype for Business Server in the Skype for Business Server forest.

Container for new shadow accounts

The Master Account Management policy allows you to specify the container in which you want Active Roles to create shadow accounts when enabling master accounts for Skype for Business Server. You can select the desired organizational unit in the Skype for Business Server forest or you can let Active Roles choose the default container.

If you select a particular organizational unit, Active Roles creates shadow accounts in that organizational unit. You can select an organizational unit from any domain of the Skype for Business Server forest that is registered with Active Roles as a managed domain.

If you let Active Roles choose the default container for new shadow aActive Rolesccounts, then Active Roles creates shadow accounts in the **Users** container in a particular domain of the Skype for Business Server forest. If the forest root domain of the Skype for Business Server forest is registered with Active Roles as a managed domain, then Active Roles creates shadow accounts in that domain. Otherwise, Active Roles creates shadow accounts in the domain that appears first in the ordered list of the managed domains from the Skype for Business Server forest. Note that Active Roles requires at least one domain of the Skype for Business Server forest to be registered with Active Roles as a managed domain.

Default description for new shadow accounts

The Master Account Management policy allows you to specify a text to use as the default description for new shadow accounts that Active Roles creates when enabling master accounts for Skype for Business Server. Active Roles writes that text to the **Description** property of every new shadow account.

Attribute to store a reference to shadow account

By default, the Master Account Management policy designates the **adminDescription** attribute of the master account for storing the GUID of the shadow account, and allows you to choose a different attribute for that purpose. Skype for Business Server User Management uses this attribute to identify the shadow account in the Skype for Business Server forest when managing a given master account in an external forest. The policy causes Active Roles to set this attribute on the master account when linking the master account to the shadow account in the Skype for Business Server forest.

Synchronized properties

The Master Account Management policy defines a list of properties to copy from the master account to the shadow account. These properties are referred to as *synchronized properties*. When you use Active Roles to set or change a synchronized property of a master account, the policy causes Active Roles to set or change the value of that property on both the master account and shadow account.

In addition, Skype for Business Server User Management provides a scheduled task that copies synchronized properties from every managed master account to the corresponding shadow account. The task runs on a scheduled basis to ensure that each of the synchronized properties of the shadow account has the same value as the corresponding property of the master account. If a synchronized property of the shadow account has changed for whatever reason, Active Roles changes that property back to the value found on the master account. For further details, see Scheduled synchronization later in this document.

The following table provides the default list of synchronized properties. You can configure the policy to synchronize additional properties or remove individual properties from synchronization.

Table 3: Default list of synchronized properties

c (Country Abbreviation)

co (Country)

company (Company)

countryCode (Country-Code)

department (Department)

displayName (Display Name)

givenName (First Name)

homePhone (Home Phone)

initials (Initials)

l (City)

mobile (Mobile Number)

otherTelephone (Phone Number (Others))

physicalDeliveryOfficeName (Office Location)

postalCode (ZIP/Postal Code)

postOfficeBox (Post Office Box)

sAMAccountName (Logon Name (pre-Windows 2000))

sn (Last Name)

st (State/Province)

streetAddress (Street Address)

telephoneNumber (Telephone Number)

title (Job Title)

url (Web Page Address (Others))

wWWHomePage (Web Page Address)

Substituted properties

The Master Account Management policy defines a list of properties that appear on the master account but reflect the properties of the shadow account. These properties are referred to as *substituted properties*. When you use Active Roles to view properties of a master account, the policy causes Active Roles to retrieve the values of the master account's substituted properties from the shadow account. When you use Active Roles to set or change a substituted property of a master account, the policy causes Active Roles to set or change the value of that property on the shadow account.

The policy does not allow you to narrow down the list of substituted properties. However, you can specify your custom list of substituted properties in addition to the default list. If you do so, the resulting list of substituted properties includes all properties from both the default list and your custom list.

Table 4: Default list of substituted properties

- edsva-Skype for Business-AccountExists
- edsva-Skype for Business-ArchivingPolicy
- edsva-Skype for Business-ClientPolicy
- edsva-Skype for Business-ClientVersionPolicy
- edsva-Skype for Business-ConferencingPolicy
- edsva-Skype for Business-DialPlanPolicy
- edsva-Skype for Business-Disable
- edsva-Skype for Business-Enable
- edsva-Skype for Business-ExchangeArchivingPolicy
- edsva-Skype for Business-ExternalAccessPolicy
- edsva-Skype for Business-HostedVoiceMail
- edsva-Skype for Business-IsEnabled
- edsva-Skype for Business-LineServerURI
- edsva-Skype for Business-LineURI
- edsva-Skype for Business-LocationPolicy
- edsva-Skype for Business-MasterAccount
- edsva-Skype for Business-MobilityPolicy
- edsva-Skype for Business-Move
- edsva-Skype for Business-MoveTargetRegistrarPool
- edsva-Skype for Business-PersistentChatPolicy
- edsva-Skype for Business-PIN
- edsva-Skype for Business-PINPolicy
- edsva-Skype for Business-PrivateLine
- edsva-Skype for Business-ReEnable
- edsva-Skype for Business-RegistrarPool
- edsva-Skype for Business-SIPAddress
- edsva-Skype for Business-SIPAddressType
- edsva-Skype for Business-SIPDomain
- edsva-Skype for Business-SIPUserName
- edsva-Skype for Business-TasksAllowed
- edsva-Skype for Business-TelephonyOption
- edsva-Skype for Business-TemporarilyDisable
- edsva-Skype for Business-VoicePolicy

Back-synchronized properties

The Master Account Management policy defines a list of properties to copy from the shadow account to the master account. By default, the list is empty. If you add a property to that list, the policy ensures that any changes to that property on the shadow account are replicated to the master account.

Master Account Management policy actions

The Master Account Management policy causes Active Roles to perform the following actions depending on the change request submitted to the Active Roles Administration Service.

Table 5: Policy Actions

Request	Actions
Enable an existing Active Directory user for Skype for Business Server	Active Roles retrieves the properties of the existing user (in the external forest), and then performs the following actions: • Create a shadow account in the Skype for Business Server forest, and populate its properties with the properties of the user from the external forest • Enable the shadow account for Skype for Business Server • Set the `msRTCSIP-OriginatorSID` attribute of the shadow account to the value of the `objectSID` attribute of the user from the external forest • Create a reference to the shadow account on the master account If the user from the external forest already has a shadow account (for example, created by Exchange Resource Forest Management), then the policy re-uses the existing shadow account instead of creating a new one. When creating the shadow account, Active Roles executes all policies that are applied to the container that holds the shadow account.
Modify Skype for Business Server user properties of a master account	If the change request includes any changes to substituted properties, Active Roles first makes the requested changes to the substituted properties of the shadow account. Next, Active Roles makes the requested changes to the properties of the master account, and then updates the synchronized properties of the shadow account with the new property values found on the master account.
Deprovision a master account	Active Roles deprovisions the master account, and then temporarily disables the shadow account for Skype for Business Server.
Undeprovision a deprovisioned master account	Active Roles undeprovisions the master account and then re-enables the shadow account for Skype for Business Server. For undeprovisioning master accounts to have an effect on shadow accounts, the container that holds deprovisioned master accounts must be in the scope of the **Built-in Policy - Skype for Business - Master Account Management** Policy Object (or a copy of that Policy Object).
Delete a master account	Active Roles deletes the master account, and then removes the shadow account from Skype for Business Server.

The Master Account Management policy requires that shadow accounts be in the scope of the User Management policy provided by Skype for Business Server User Management.

This enables Active Roles to perform the Skype for Business Server related actions on the shadow account.

Scheduled synchronization

Skype for Business Server User Management includes an Active Roles scheduled task that complements the Master Account Management policy to enforce synchronization of master and shadow account properties, and to capture existing Skype for Business Server users whose master account happens to fall under the control of that policy. The scheduled task object is in the **Configuration/Server Configuration/Scheduled Tasks/Builtin** container. The name of the object is **Skype for Business - Master Account Management**. The task is scheduled to run on a daily basis. Normally, you do not need to modify that scheduled task.

The operation of the task affects only the user accounts that are in the scope of the **Built-in Policy - Skype for Business - Master Account Management** Policy Object (or a copy of that Policy Object). When run, the task performs the following actions on each of those user accounts:

- If the user account does not have a shadow account that is enabled for Skype for Business Server, then skip over that user account.
- If the user account has a shadow account that is enabled for Skype for Business Server but does not store a reference to that shadow account, then create the reference to the shadow account on that user account.

  This action enables Skype for Business Server User Management to administer exiting Skype for Business Server users, possibly enabled for Skype for Business Server by using an earlier version of Skype for Business Server User Management or without the use of Skype for Business Server User Management.
- If the user account has a shadow account that is enabled for Skype for Business Server and stores a reference to the shadow account, then copy the synchronized properties from the master account to the shadow account, and copy the back-synchronized properties from the shadow account to the master account.

  This action ensures that the shadow account properties are updated with the latest changes to the master account properties and vice versa.

Access Templates for Skype for Business Server

Skype for Business Server User Management provides a number of Access Templates allowing you to delegate the tasks of managing Skype for Business Server users in Active Roles. You can find these Access Templates in the **Configuration/Access Templates/Skype for Business Server** container:

Table 6: Skype for Business Server User Management Access

Access Template	Description
Skype for Business Server - User Full Control	Gives permission to perform the following tasks by using Active Roles: • Add and enable new Skype for Business Server users • View existing Skype for Business Server users • View or change the SIP address • View or change the telephony option and related settings • View or change the user policy assignments in Skype for Business Server • Temporarily disable or re-enable users for Skype for Business Server • Move users to another server or pool in Skype for Business Server • Remove users from Skype for Business Server
Skype for Business Server - User Telephony	Gives permission to perform the following tasks by using Active Roles: • View existing Skype for Business Server users • View the SIP address • View or change the telephony option and related settings • View the user policy assignments in Skype for Business Server
Skype for Business Server - User Disable/Re-enable	Gives permission to perform the following tasks by using Active Roles: • View existing Skype for Business Server users • View the SIP address • View the telephony option and related settings • View the user policy assignments in Skype for Business Server • Temporarily disable or re-enable users for Skype for Business Server
Skype for Business Server - User Policies	Gives permission to perform the following tasks by using Active Roles:

Access Template	Description
	• View existing Skype for Business Server users • View the SIP address • View the telephony option and related settings • View or change the user policy assignments in Skype for Business Server

When applying Access Templates for Skype for Business Server User Management, consider your Active Directory topology.

Table 7: Applying Access templates for Skype for Business Server User Management

Topology option	Where to apply Access Templates
Single forest	Apply Access Templates to Active Directory domains and containers to which the **Built-in Policy - Skype for Business - User Management** Policy Object (or a copy of that Policy Object) is applied, to allow access to user accounts of Skype for Business Server users managed by Active Roles.
Multiple forests - Resource forest	Apply Access Templates to Active Directory domains and containers in external forests to which the **Built-in Policy - Skype for Business - Master Account Management** Policy Object (or a copy of that Policy Object) is applied, to allow access to master accounts of Skype for Business Server uses managed by Active Roles. You do not need to apply these Access Templates in the Skype for Business Server forest.
Multiple forests - Central forest	Apply Access Templates to Active Directory domains and containers in external forests to which the **Built-in Policy - Skype for Business - Master Account Management** Policy Object (or a copy of that Policy Object) is applied, to allow access to master accounts of Skype for Business Server uses managed by Active Roles. Apply Access Templates to Active Directory domains and containers in the Skype for Business Server forest to which the **Built-in Policy - Skype for Business - User Management** Policy Object (or a copy of that Policy Object) is applied, to allow access to logon-enabled user accounts of Skype for Business Server users managed by Active Roles in the Skype for Business Server forest.

Deploying the Solution

Prerequisite conditions

This section summarizes the prerequisite conditions that must be met before you deploy Skype for Business Server User Management.

Skype for Business Server deployment

With Skype for Business Server User Management, you can perform user management on Microsoft Lync 2010 or Microsoft Lync 2013.

Single forest

In case of single forest, Skype for Business Server must be deployed in the forest that holds logon-enabled accounts for Skype for Business Server users. For further details, see Single forest earlier in this document.

Multiple forests

In case of multiple forests, Skype for Business Server must be deployed in the Skype for Business Server forest only. You don't need to deploy Skype for Business Server in external user forests or extend the Active Directory schema with Skype for Business Server attributes in those forests. For further details about multi-forest topology options,

see Multiple forests - Resource forest and Multiple forests - Central forest earlier in this document.

Active Directory forest trust

The multi-forest topology option requires a one-way trust relationship between the Skype for Business Server forest and each user forest so that users can authenticate to the user forest but access services in the Skype for Business Server forest. Create a "forest" trust instead of an "external" trust because an external trust only supports NTLM, while a forest trust supports both NTLM and Kerberos, and therefore won't limit Skype for Business client authentication options.

Trusts are configured as one-way to prevent unauthorized access to the user forest from the Skype for Business Server forest. For details, see "How Domain and Forest Trusts Work" at http://technet.microsoft.com/library/cc773178.aspx.

Skype for Business Server contact management rights

In case of central forest deployment, you need to grant Skype for Business Server contact management rights on the container that is intended to hold shadow accounts (contacts enabled for Skype for Business Server in the Skype for Business Server forest). Otherwise, Skype for Business Server security groups do not have sufficient rights to manage contact objects, which causes an "access is denied" condition when Active Roles attempts to enable a shadow account for Skype for Business Server.

To grant Skype for Business Server contact management rights, use the following command in Skype for Business Server Management Shell:

```
Grant-CsOUPermission -OU "<DN of container>" -ObjectType "contact"
```

Replace `<DN of container>` with the Distinguished Name of the container that is intended to hold shadow accounts, for example: `OU=Shadow Accounts,DC=Skype for BusinessServer,DC=lab`. If the domain does not have permission inheritance disabled (which is the default case), then you can supply the Distinguished Name of the domain rather than container:

```
Grant-CsOUPermission -OU "DC=Skype for BusinessServer,DC=lab" -ObjectType "contact"
```

You must be a domain administrator in order to run the `Grant-CsOUPermission` cmdlet locally.

Active Roles deployment

The following Active Roles components must be installed in your Active Directory environment:

- Administration Service
- Web Interface
- Active Roles console

You can install these components on member servers in a user forest or in the Skype for Business Server forest. For installation instructions, see the Active Roles Quick Start Guide.

Log on as Active Roles Admin

To configure Skype for Business Server User Management, log on as Active Roles Admin. This ensures that you have sufficient rights to make the necessary configuration changes. Assuming the default configuration of the Active Roles Administration Service, you should log on with a domain user account that is a member of the Administrators group on the computer running the Administration Service.

Register domains with Active Roles

Skype for Business Server User Management requires the following domains to be registered with Active Roles:

- At least one domain that holds computers running the Front End Server or Standard Edition Server role in your Skype for Business Server deployment
- Domains that hold logon-enabled users you are going to administer with Skype for Business Server User Management
- In case of multi-forest topology, the domain in the Skype for Business Server forest that holds shadow accounts for Skype for Business Server users

When registering a domain, you are prompted to choose which account you want the Administration Service to use to access the domain. You can either specify a so-called *override account* or let the Administration Service use its service account. With either option, the account must have sufficient rights in the domain you are registering. At a minimum, the account must have the following rights:

- In the domain that holds Skype for Business Server computers, a member of the **RTCUniversalUserAdmins** group
- In the user domains, a member of the **Account Operators** group
- In the shadow accounts domain, a member of the **Account Operators** group

  For a central forest deployment, the account must also have the rights to create, view, modify and delete contact objects in the shadow accounts domain. It will suffice to make the account a member of the **Domain Admins** group.

  For instructions on how to register domains with Active Roles, see "Adding and removing managed domains" in the Active Roles Administrator Guide.

Deployment in a single-forest environment

In a single-forest environment, you only need to link the **Built-in Policy - Skype for Business - User Management** Policy Object to the Active Directory domains or containers that hold user accounts for which you want Active Roles to perform Skype for Business Server user management tasks.

To link the Policy Object to an organizational unit or domain

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Builtin**.
2. In the details pane, right-click the **Built-in Policy - Skype for Business - User Management** Policy Object, and then click **Policy Scope**.
3. In the dialog box that appears, click **Add**, and then select the desired organizational unit or domain.

Out of the box, the Policy Object has all policy settings configured. You can use the Active Roles console to view or change policy settings as needed.

To view or change policy settings

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Builtin**.
2. In the details pane, double-click the **Built-in Policy - Skype for Business - User Management** Policy Object.
3. In the **Properties** dialog box that appears, go to the **Policies** tab, and double-click the entry in the list of policies.
4. In the **Properties** dialog box that appears, do any of the following:
    - On the **Server** tab, specify how you want Active Roles to select a computer running Skype for Business Server.
    - On the **SIP User Name** tab, configure a rule for generating the SIP user name in the user SIP address.
    - On the **SIP Domain** tab, configure a rule to restrict selection of a SIP domain for the user SIP address.
    - On the **Pool** tab, configure a rule to restrict selection of an Enterprise Edition Front End pool or Standard Edition server to which Skype for Business Server users can be assigned.
    - On the **Telephony** tab, configure a rule to restrict selection of a Telephony option for Skype for Business Server users.

For detailed description of the policy settings, see User Management policy settings earlier in this document.

Deployment in a multi-forest environment

In a multi-forest environment, you need to perform the following deployment tasks:

- Apply the Master Account Management policy Adjust the **Forest Mode** policy setting in the **Built-in Policy - Skype for Business - Master Account Management** Policy Object and then link that Policy Object to Active Directory domains or containers that hold logon-enabled user accounts in user forests (master accounts) for which you want Active Roles to perform Skype for Business Server user management tasks.
- Apply the User Management policy Link the **Built-in Policy - Skype for Business - User Management** Policy Object to Active Directory domains or containers in the Skype for Business Server forest that hold shadow accounts.

  In case of central forest, you also need to link the **Built-in Policy - Skype for Business - User Management** Policy Object to Active Directory domains or containers in the Skype for Business Server forest that hold logon-enabled user accounts for which you want Active Roles to perform Skype for Business Server user management tasks.

Apply the Master Account Management policy

The **Built-in Policy - Skype for Business - Master Account Management** Policy Object enables Active Roles to perform Skype for Business Server user management tasks on user accounts in Active Directory forests that are external to the Skype for Business Server forest. It needs to be configured as appropriate to your Skype for Business Server forest mode (resource forest or central forest) and then linked to domains or containers in external user forests.

To configure the Policy Object

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Builtin**.
2. In the details pane, double-click the **Built-in Policy - Skype for Business - Master Account Management** Policy Object.
3. In the **Properties** dialog box that appears, go to the **Policies** tab, and double-click the entry in the list of policies.
4. In the **Properties** dialog box that appears, go to the **Forest Mode** tab and select the option that matches the Skype for Business Server forest mode in your Skype for Business Server deployment (see Skype for Business Server forest mode).

5. Review other policy settings:
    - On the **Shadow Account** tab, view or change the container and default description for new shadow accounts.
    - On the **Master Account** tab, view or change the attribute to store a reference to shadow account.
    - On the **Synced** tab, view or change the list of synchronized properties.
    - On the **Substituted** tab, configure your custom list of substituted properties in addition to the default list.
    - On the **Back-synced** tab, view or change the list of back-synchronized properties.

For detailed description of the policy settings, see Master Account Management policy settings earlier in this document.

To link the Policy Object to an organizational unit or domain

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Builtin**.
2. In the details pane, right-click the **Built-in Policy - Skype for Business - Master Account Management** Policy Object, and then click **Policy Scope**.
3. In the dialog box that appears, click **Add**, and then select the desired organizational unit or domain.

Apply the User Management policy

The **Built-in Policy - Skype for Business - User Management** Policy Object enables Active Roles to perform Skype for Business Server user management tasks on user accounts in the Skype for Business Server forest. It needs to be linked to domains or containers in the Skype for Business Server forest that hold shadow accounts. In case of central forest, you also need to link that Policy Object to Active Directory domains or containers in the Skype for Business Server forest that hold logon-enabled user accounts for which you want Active Roles to perform Skype for Business Server user management tasks.

To link the Policy Object to an organizational unit or domain

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Builtin**.
2. In the details pane, right-click the **Built-in Policy - Skype for Business - User Management** Policy Object, and then click **Policy Scope**.
3. In the dialog box that appears, click **Add**, and then select the desired organizational unit or domain.

Out of the box, the Policy Object has all policy settings configured. You can use the Active Roles console to view or change policy settings as needed.

To view or change policy settings

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Builtin**.
2. In the details pane, double-click the **Built-in Policy - Skype for Business - User Management** Policy Object.
3. In the **Properties** dialog box that appears, go to the **Policies** tab, and double-click the entry in the list of policies.
4. In the **Properties** dialog box that appears, do any of the following:
    - On the **Server** tab, specify how you want Active Roles to select a computer running Skype for Business Server.
    - On the **SIP User Name** tab, configure a rule for generating the SIP user name in the user SIP address.
    - On the **SIP Domain** tab, configure a rule to restrict selection of a SIP domain for the user SIP address.
    - On the **Pool** tab, configure a rule to restrict selection of an Enterprise Edition Front End pool or Standard Edition server to which Skype for Business Server users can be assigned.
    - On the **Telephony** tab, configure a rule to restrict selection of a Telephony option for Skype for Business Server users.

For detailed description of the policy settings, see User Management policy settings earlier in this document.

Upgrade from an earlier version

You can use the following steps to upgrade from Active Roles Add-on for Skype for Business Server to Skype for Business Server User Management:

1. Identify the Active Directory topology option used by the add-on. The possible options are:
    - Single forest
    - Multiple forests - Resource forest
    - Multiple forests - Central forest

    In case of multiple forests, note down the Distinguished Name of the container in which the add-on creates shadow accounts.
2. Uninstall the earlier version of the add-on from Active Roles Add-on Manager, and then uninstall the add-on from the system
3. Upgrade to Active Roles version 7.2. For upgrade instructions, see the Active Roles 7.2 Quick Start Guide.
4. Deploy Skype for Business Server User Management. Depending on the Active Directory topology option used by the add-on:

- In case of single forest, follow the Deployment in a single-forest environment instructions.
- In case of multiple forests, follow the Deployment in a multi-forest environment instructions. Configure the **Built-in Policy - Skype for Business - Master Account Management** Policy Object to match the topology option and container for shadow accounts you identified in Step 1.

The following instructions elaborate on these steps. The instructions apply to Active Roles Add-on for Skype for Business Server 2.1.

To identify the Active Directory topology option used by the add-on

1. In the Active Roles console tree, select **Applications | Active Roles Add-on for Skype for Business Server**.
2. Review the add-on settings in the **Configure Add-on** area in the details pane:
   - The Active Directory topology option is selected in the **Active Directory topology** box.
   - If a multi-forest option is selected, the Distinguished Name of the container in which the add-on creates shadow accounts is specified in the **Container for shadow accounts/contacts** box.

If the add-on was configured with the resource forest or central forest option, you need to configure and apply the **Built-in Policy - Skype for Business - Master Account Management** Policy Object as follows.

To configure and apply the Master Account Management policy

1. In the Active Roles console tree, select **Configuration | Policies | Administration | Builtin**.
2. In the details pane, double-click the **Built-in Policy - Skype for Business - Master Account Management** Policy Object.
3. In the **Properties** dialog box that appears, go to the **Policies** tab, and double-click the entry in the list of policies.
4. In the **Properties** dialog box that appears, go to the **Forest Mode** tab and select the option that matches the Active Directory topology option that was used by the add-on:
   - If the add-on was configured with the option **Multiple forests - Resource forest**, then select the **Resource forest** option on the **Forest Mode** tab.
   - If the add-on was configured with the option **Multiple forests - Central forest**, then select the **Central forest** option on the **Forest Mode** tab.
5. Go to the **Shadow Account** tab and configure the policy to use the container for shadow accounts that was used by the add-on: Click **This container**, click **Browse**, and select the container.
6. Click **OK** to close the **Properties** dialog for the policy entry.
7. In the **Properties** dialog box for the Policy Object, click **Apply**, go to the **Scope** tab, and then click the **Scope** button on that tab.

8. In the dialog box that appears, add the containers that hold the master accounts you managed using the add-on, and then click **OK**.
9. Click **OK** to close the **Properties** dialog box for the Policy Object.

Skype for Business Server User Management recognizes the existing master accounts, enabling Active Roles to manage their shadow accounts for Skype for Business Server in the same way as when using the add-on. To expedite the recognition of the existing master accounts, you might execute the Master Account Management task without waiting for its scheduled run: In the Active Roles console, navigate to the **Configuration/Server Configuration/Scheduled Tasks/Builtin** container, right-click the object **Skype for Business - Master Account Management** in that container, point to **All Tasks**, and then click **Execute**.

3

Managing Skype for Business Server Users

The Skype for Business Server User Management solution enables Active Roles to administer Skype for Business Server users. Once you have deployed Skype for Business Server User Management, the Active Roles Web Interface can be used to perform the following tasks:

- Enabling or disabling users for Skype for Business Server
- Managing Skype for Business Server user properties

Enabling or disabling users for Skype for Business Server

By using the Active Roles Web Interface, you can enable, temporarily disable, or remove Active Directory users from Skype for Business Server.

Add and enable a new Skype for Business Server user

For an existing Active Directory user account, you can use the Active Roles Web Interface to create and enable a new Skype for Business Server user account by adding the Active Directory user to Skype for Business Server.

To add and enable a new Skype for Business Server user

1. Select the user account in the Active Roles Web Interface for administrators.
2. Click the **Enable for Skype for Business Server** command.

   The command is available if you have sufficient rights in Active Roles to enable users for Skype for Business Server, and the selected account is in the scope of the policy

provided by Skype for Business Server User Management and is not enabled for Skype for Business Server; otherwise, the Web Interface does not display the **Enable for Skype for Business Server** command.

3. On the page that appears, assign the user to a Skype for Business Server pool, specify any additional details, assign Skype for Business Server policies to the user as needed, and then click **Finish**.

Disable or re-enable a user account for Skype for Business Server

You can use the Active Roles Web Interface to disable a user account for logon to Skype for Business Server. This allows you to disable a previously enabled user account in Skype for Business Server while retaining all the Skype for Business Server settings that were configured for the user account. Because you do not lose the Skype for Business Server user account settings, you can re-enable a disabled user account again without having to reconfigure the user account.

To disable or re-enable a previously enabled user account for Skype for Business Server

1. In the Active Roles Web Interface for administrators, select the user account that you want to disable or re-enable.
2. Do one of the following:
    - To disable the user account, click the **Temporarily Disable for Skype for Business Server** command.
    - To re-enable the user account, click the **Re-enable for Skype for Business Server** command.

The Web Interface displays the **Temporarily Disable for Skype for Business Server** command if you have sufficient rights in Active Roles to perform that command, and the user account you have selected is in the scope of the policy provided by Skype for Business Server User Management and is enabled for Skype for Business Server.

The Web Interface displays the **Re-enable for Skype for Business Server** command if you have sufficient rights in Active Roles to perform that command, and the user account you have selected is in the scope of the policy provided by Skype for Business Server User Management and was disabled by using the **Temporarily Disable for Skype for Business Server** command.

Remove a user account from Skype for Business Server

You can use the Active Roles Web Interface to remove a user account from Skype for Business Server. This removes all the Skype for Business Server related attributes from the user account, including the identities of any per-user policies that have been assigned to that user account. You can later re-add the account to Skype for Business Server by using the **Enable for Skype for Business Server** command (see Add and enable a new Skype for Business Server user). However, all the Skype for Business Server-related information (including policy assignments) previously associated with that account will have to be re-created. If you want to prevent a user from logging on to Skype for Business Server, but do not want to lose all of their account information, you can temporarily disable the user account for Skype for Business Server (see Disable or re-enable a user account for Skype for Business Server).

To remove a user account from Skype for Business Server

1. In the Active Roles Web Interface for administrators, select the user account that you want to remove from Skype for Business Server.
2. Click the **Remove from Skype for Business Server** command.

The Web Interface displays the **Remove from Skype for Business Server** command if you have sufficient rights in Active Roles to perform that command, and the user account you have selected is in the scope of the policy provided by Skype for Business Server User Management and is enabled or temporarily disabled for Skype for Business Server.

Managing Skype for Business Server user properties

By using the Active Roles Web Interface, you can:

- View or change Skype for Business Server user properties such as the user's SIP address, telephony options and Skype for Business Server policy assignments
- Move Skype for Business Server users to a different Enterprise Edition Front End pool or Standard Edition server

View or change Skype for Business Server user properties

For a user account that is enabled or temporarily disabled for Skype for Business Server, you can use the Active Roles Web Interface to view or change Skype for Business Server

user properties such as the user's SIP address, telephony options and Skype for Business Server policy assignments.

To view or change Skype for Business Server user properties

1. In the Active Roles Web Interface for administrators, select the user account whose properties you want to view or change.
2. Click the **Skype for Business Server User Properties** command.

   The Web Interface displays the **Skype for Business Server User Properties** command if you have sufficient rights in Active Roles to view Skype for Business Server user properties of the selected account, and the user account you have selected is in the scope of the policy provided by Skype for Business Server User Management and is enabled or temporarily disabled for Skype for Business Server.
3. On the page that appears, view or change the following settings:
   - **Enabled for Skype for Business Server** Indicates whether or not the user is enabled to log on to Skype for Business Server. If you clear this check box, the user will no longer be able to log on to Skype for Business Server. Selecting this check box re-enables the user to log on to Skype for Business Server. The function of this check box is equivalent to the **Temporarily Disable for Skype for Business Server** and **Re-enable for Skype for Business Server** commands (see Disable or re-enable a user account for Skype for Business Server).
   - **SIP address** Indicates the user's SIP address (SIP URI), a unique identifier that allows the user to communicate using SIP devices such as Microsoft Skype for Business. The SIP address consists of the SIP user name on the left side of the @ symbol, and the SIP domain name on the right side. It must be prefaced by "sip:"; for example, sip:John.Smith@company.com.
   - **Registrar pool** Identifies the Enterprise Edition Front End pool or Standard Edition server where the Skype for Business Server user is homed. If you need to move the user to a different server or pool, see Move a user to another server or pool in Skype for Business Server later in this document.
   - **Telephony** Specifies whether the Skype for Business Server user can make PC-to-PC calls with audio and video, route incoming and outgoing calls, and control the desktop phone. The possible telephony options are as follows:
     - **PC-to-PC only** The user can make only PC-to-PC audio or video calls.
     - **Audio/video disabled** The user cannot make calls with audio and video.
     - **Remote call control** The user can use Skype for Business Server to control the desktop phone, and can also make PC-to-PC calls.
     - **Enterprise Voice** The user can use Skype for Business Server to route all incoming and outgoing calls, and can also make PC-to-PC calls.
     - **Remote call control only** The user can use Skype for Business Server to control the desktop phone, but cannot make PC-to-PC audio calls.

- **Line URI** Applies to all telephony options but **Audio/video disabled**. Specifies the primary phone number assigned to the Skype for Business Server user.

  The line URI must use the E.164 format and have the "TEL:" prefix. For example: TEL:+12345678997. The extension number, if any, should be added at the end of the line URI, for example: TEL:+12345678997;ext=65431.
- **Line server URI** Applies to the **Remote call control** and **Remote call control only** options. Specifies the URI of the remote call control telephone gateway assigned to the Skype for Business Server user.

  The line server URI is the gateway URI, prefaced by “sip:”; for example, sip:rccgateway@company.com.
- **Dial plan policy** Applies to the **Enterprise Voice** option. Identifies the dial plan currently assigned to the Skype for Business Server user, and allows you to assign a different dial plan.
- **Voice policy** Applies to the **Enterprise Voice** option. Identifies the voice policy currently assigned to the Skype for Business Server user, and allows you to assign a different voice policy.
- **Conferencing policy** Identifies the conferencing policy currently assigned to the Skype for Business Server user, and allows you to assign a different conferencing policy to the user.
- **Conferencing policy** Identifies the conferencing policy currently assigned to the Skype for Business Server user, and allows you to assign a different conferencing policy to the user.
- **Client version policy** Identifies the client version policy currently assigned to the Skype for Business Server user, and allows you to assign a different client version policy.
- **PIN policy** Identifies the personal identification number (PIN) policy currently assigned to the Skype for Business Server user, and allows you to assign a different PIN policy.
- **External access policy** Identifies the external access policy currently assigned to the Skype for Business Server user, and allows you to assign a different external access policy.
- **Archiving policy** Identifies the archiving policy currently assigned to the Skype for Business Server user, and allows you to assign a different archiving policy.
- **Location policy** Identifies the location policy currently assigned to the Skype for Business Server user, and allows you to assign a different location policy.
- **Mobility policy** Identifies the mobility policy currently assigned to the Skype for Business Server user, and allows you to assign a different mobility policy.
- **Persistent Chat policy** Identifies the persistent chat policy currently assigned to the Skype for Business Server user, and allows you to assign a different persistent chat policy.

- **Client policy** Identifies the client policy currently assigned to the Skype for Business Server user, and allows you to assign a different client policy.

Skype for Business Server user account properties allow you to assign certain policies to a Skype for Business Server user in order to specify particular settings that differ from the settings defined in policies assigned to other users, such as global policies. These policies are referred to as user policies.

In Skype for Business Server, deploying and assigning user policies is optional. It is possible to deploy only global policies or site policies. If user policies are deployed, they must be assigned to users explicitly. When managing Skype for Business Server user settings, you can select the appropriate user policy from a list. The list also includes the **<Automatic>** entry. If **<Automatic>** is selected, the global policy (or, if defined, the site policy) is assigned to the user.

Move a user to another server or pool in Skype for Business Server

For a user account that is enabled or temporarily disabled for Skype for Business Server, you can use the Active Roles Web Interface to move the user account to a specific Enterprise Edition Front End pool or Standard Edition server.

To move a Skype for Business Server user account to a different server or pool

1. In the Active Roles Web Interface for administrators, select the user account you want to move.
2. Click the **Move to Skype for Business Server Pool** command.

   The Web Interface displays the **Move to Skype for Business Server Pool** command if you have sufficient rights in Active Roles to perform that command, and the user account you have selected is in the scope of the policy provided by Skype for Business Server User Management and is enabled or temporarily disabled for Skype for Business Server.
3. On the page that appears, select the server or pool to which you want to move the Skype for Business Server user.
4. Click **Finish**.

About us

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

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