

Last Modified: September 14, 2015

Citrix OpenVoice provides high-quality, easy-to-use audio conferencing services for business of all sizes.

Before You Begin

- Acquire an administrator account to RSA SecurID Access.
- Acquire an administrator account to GoToMeeting with the OpenVoice feature.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.


Procedure

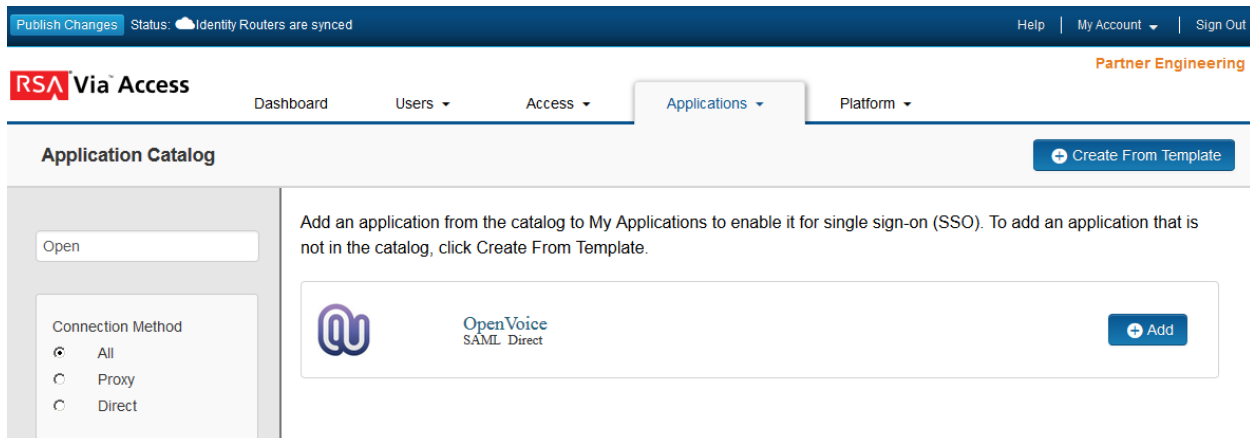
1. [Add the Application in RSA SecurID Access](#)
2. [Configure OpenVoice to Use RSA SecurID Access as an Identity Provider](#)

Add the Application in RSA SecurID Access

Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, search for **OpenVoice** and click **+Add**.

 **Note:** Refer to GoToMeeting if you want a single application in the portal to access all the Citrix Online features.



The screenshot shows the RSA SecurID Access Administration Console interface. At the top, there is a navigation bar with "Publish Changes", "Status: Identity Routers are synced", "Help", "My Account", and "Sign Out". Below this is the "RSA Via Access" header with a "Partner Engineering" badge. The main navigation includes "Dashboard", "Users", "Access", "Applications" (selected), and "Platform". The "Application Catalog" section is active, featuring a search box with "Open" entered and a "Create From Template" button. A sidebar on the left shows "Connection Method" options: "All" (selected), "Proxy", and "Direct". The main content area displays a card for "OpenVoice SAML Direct" with an "Add" button. A note above the card reads: "Add an application from the catalog to My Applications to enable it for single sign-on (SSO). To add an application that is not in the catalog, click Create From Template."

3. On the Basic Information page, specify the application name and click **Next Step**.
4. On the Connection Profile page, select **IDP-initiated**.

Connection URL

IDP-initiated SP-initiated

5. Scroll down to the **SAML Identity Provider (Issuer)** section.

SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

- Default (idp_id): qek1t2wtl6qf
 Override

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

private.key

Include Certificate in Outgoing Assertion

No certificate loaded

- a. Select **Override** under Issuer Entity ID and replace the **<IDP_URL>** with your Identity Provider hostname. In this example, **portal.sso.pe-lab.com** is the hostname.
https://portal.sso.pe-lab.com/IdPServlet?idp_id=gotomeeting
- b. Select **Choose File** and upload the private key.

6. Scroll down to the **Service Provider** section.

Service Provider

Assertion Consumer Service (ACS) URL

<https://login.citrixonline.com/saml/global.openvoice.com/acs>

Audience (Service Provider Entity ID)

<https://login.citrixonline.com/saml/sp>

- a. In the **Assertion Consumer Service (ACS) URL** field, enter the following URL <https://login.citrixonline.com/saml/global.openvoice.com/acs>
- b. In the **Audience (Service Provider Entity ID)** field, enter the following URL <https://login.citrixonline.com/saml/sp>

7. Scroll down to **User Identity** section. Set the Identifier Type to **Email** and Property to **mail**.

User Identity

Name ID

Identifier Type

Email Address

User Store

PE_AD

Property

mail

⌵ Show Advanced Configuration

8. Click **Next Step**.

9. On the **User Access** page, select the desired user policy from the drop down list.

All fields are required (except where noted)

User Access

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy

No Access Allowed

Cancel

Next Step →


10. Click **Next Step**.

11. On the **Portal Display** page, select **Display in Portal**.

12. Click **Save and Finish**.

13. Click **Publish Changes**. Your application is now enabled for SSO.

Publish Changes

Status:  Changes Pending

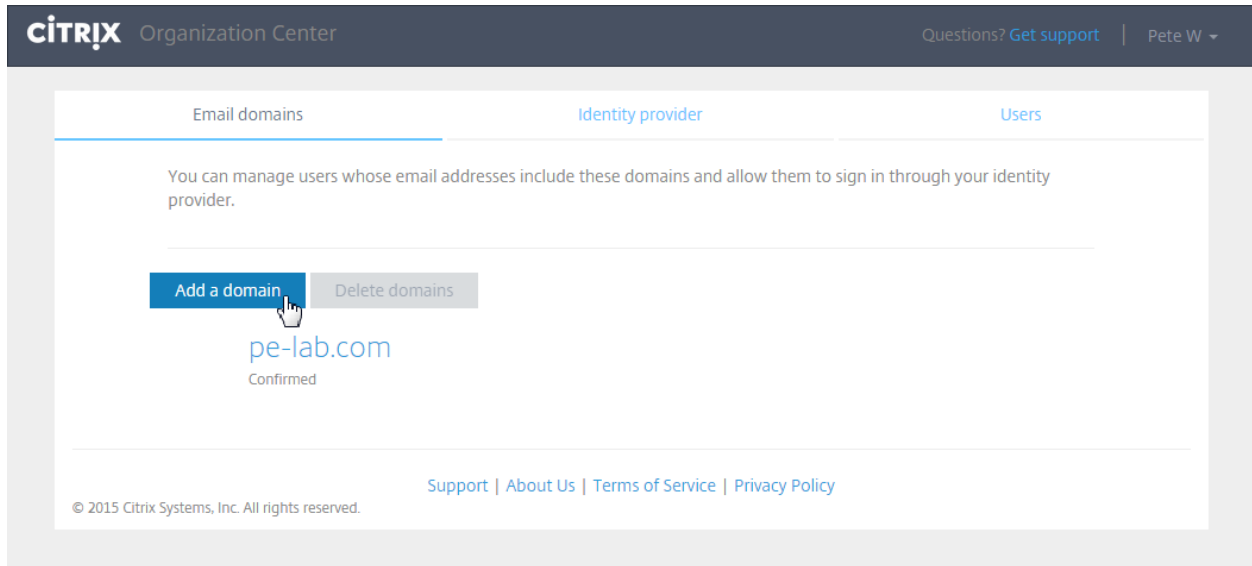
Next Steps

[Configure OpenVoice to Use RSA SecurID Access as an Identity Provider](#)

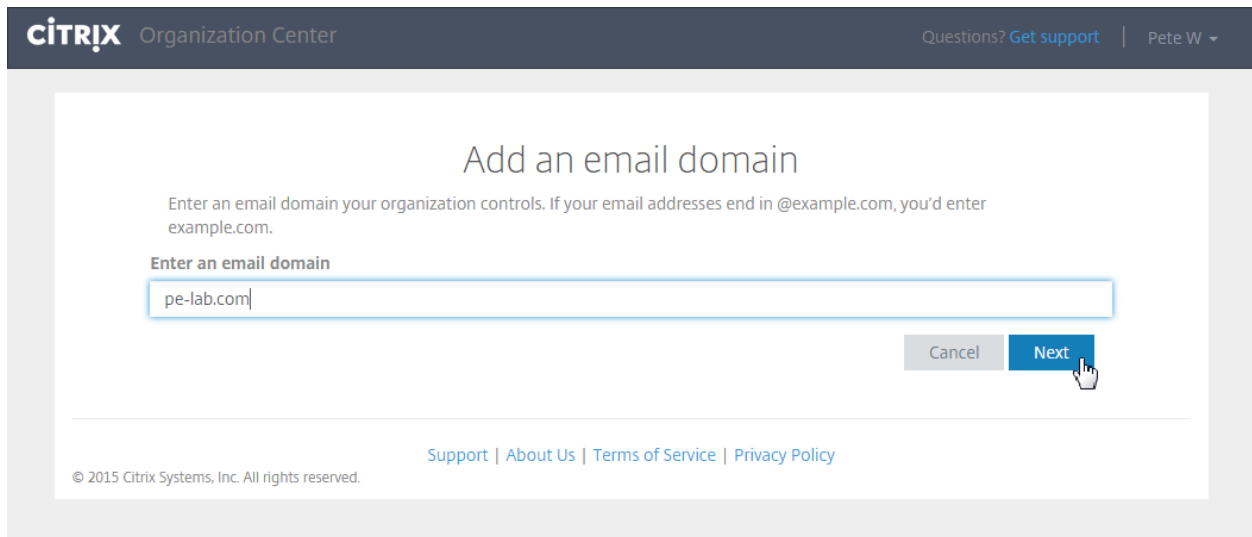
Configure OpenVoice to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login into the [Citrix Organization Center](#).
2. From the Email domains tab, click to **Add a domain**.



3. Enter the **email domain** for which you are enabling SSO with RSA SecurID Access and click **Next**.



4. Complete the verification instructions and click **Verify**.

CITRIX Organization Center Questions? [Get support](#) | Pete W ▾

Verify that you own **pe-lab.com**


Choose a method and verify that you own this email domain. If you run out of time, we'll give you new verification codes.

Method 1: Add this DNS record your domain zone file.

Name: pe-lab.com.
Type: txt
Value: citrix-verification-code=89a458e9-fd54-413d-9a45-90952f27ed8c

Method 2: Upload a file at this website.

Location: <http://pe-lab.com/citrix-verification-code.txt>
Contents: citrix-verification-code=89a458e9-fd54-413d-9a45-90952f27ed8c

Cancel Verify 

5. Open the **Identity provider** tab, select **Manual** from the drop-down menu, enter the identity provider settings and click **Save**.

CITRIX Organization Center

Email domains Identity provider Users

To allow your users to log into Citrix products using sign in credentials you manage, you can configure your Identity Provider below. Once configured, your users can log in either from the identity provider's website or from your Citrix product's website using the 'Use my company ID' link in the sign in form.

Manual

Sign-in page url
https://portal.sso.pe-lab.com/IdPServlet?idp_id=gotomeeting

Sign-out page url (optional)
Enter sign-out page url

Identity Provider Entity ID
https://portal.sso.pe-lab.com/IdPServlet?idp_id=gotomeeting

Verification certificate

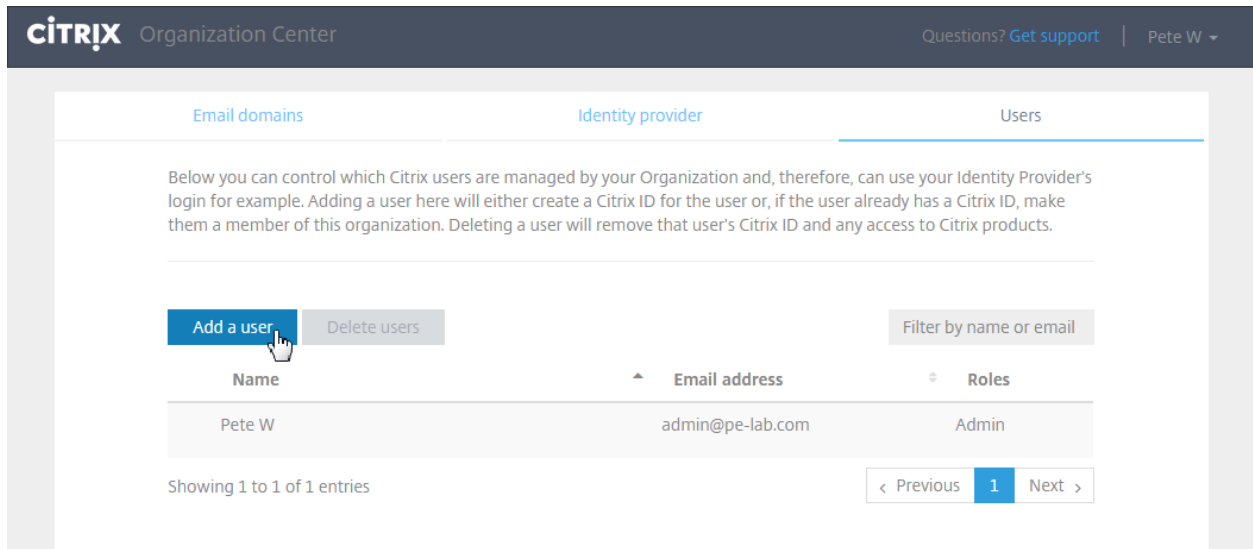
```
-----BEGIN CERTIFICATE-----
MIICrTCCAZUCBgFAT+Rz7TANBgqhkiG9w0BAQsFADAAMRgwFgYDVQQDDA9zYWxl
c2ZvcmlX3NhbWwwHhcNMTMwODA1MTkxMTQ2WhcNMTcwODA1MTkxMTQ2WjAaMRgw
FgYDVQQDDA9zYWxlC2ZvcmlX3NhbWwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQC3wyfUcGYvmpZCip8K75T+m3DxNMCe9fGCKcpZwQS7P3mPlrOfyot
RRW0Ul+Rcka/CG53Llv+wthl17MnPb5W19Vv+0SXxk1kGGhMKC/AfBMX5arXiXP
-----
```

Upload certificate

Delete Save

- The Sign-in page url is the Identity Provider URL from the SAML Identity Provider section of the RSA SecurID Access Application page.
- The Identity Provider Entity ID is the Issuer Entity ID from the SAML Identity Provider section of the RSA SecurID Access Application page
- Upload or copy/paste the public certificate.

6. Open the **Users** tab and click **Add a user**.



7. Configure the user settings and click **Save**.

