This guide describes how to create and manage user credentials on Windows VMs running on Compute Engine.

To create credentials, access the **Manage Windows Credentials** dialog:

1. In the Cloud Explorer, right-click the VM on which you want to create the credentials.
2. Select **Manage Windows Credentials**.
3. Click **Add Credentials**.
4. Enter a **Username**.
5. Enter a password, or have Visual Studio create one.
6. Click **Save**.

These credentials are encrypted on your machine and associated with the Windows VM for which they were created.

If the account already exists, having Visual Studio create a password resets the existing password. Resetting the
ord can cause the loss of encrypted data secured with the current password, including files and stored passwords. l
/compute/docs/instances/windows/creating-passwords-for-windows-instances).

To delete existing credentials, access the **Manage Windows Credentials** dialog:

1. In the Cloud Explorer, right-click the VM with the credentials you want to delete.
2. Select **Manage Windows Credential**.
3. Select a user and click **Delete credentials**.
4. Click **Delete**.

tant: Deleting credentials will delete the Windows account and the data associated with the account.

You can use the stored Windows credentials when creating a `.publishsettings` file for publishing to a VM or when starting a new Terminal Services session with the VM.

To create a `.publishsettings` file to deploy your ASP.NET app to a VM:

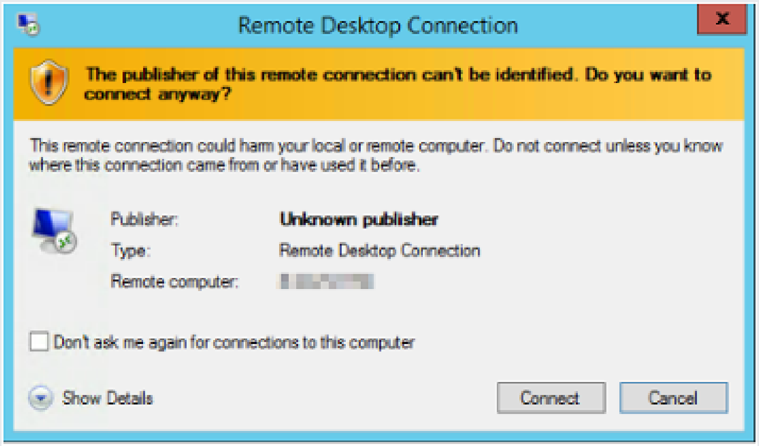
1. In the Cloud Explorer, right-click the VM where you want to deploy.
2. Select **Save publishing settings**.
3. Select the credentials to use when creating the `.publishsettings` file.
    a. If you do not see the credentials you want to use, then click **Manage Windows Credentials** to create new credentials (#creating_windows_credentials).

tant: The credentials stored in `.publishsettings` are in plain text. You should delete this file after it is imported into profile and no longer needed. The publish profile stores the credentials encrypted.

To access a VM through a remote desktop:

1. In the Cloud Explorer, right-click the VM to which you want to connect.
2. Select **Open Remote Desktop session**.
3. Select the credentials you want to use to connect to the remote desktop session.
    a. If you do not see the credentials you want to use, then click **Manage Windows Credentials** to create new credentials (#creating_windows_credentials).

You might see warnings indicating that the publisher of the remote connection can't be identified.



Remote Desktop Connection

The publisher of this remote connection can't be identified. Do you want to connect anyway?

This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.

Publisher: **Unknown publisher**

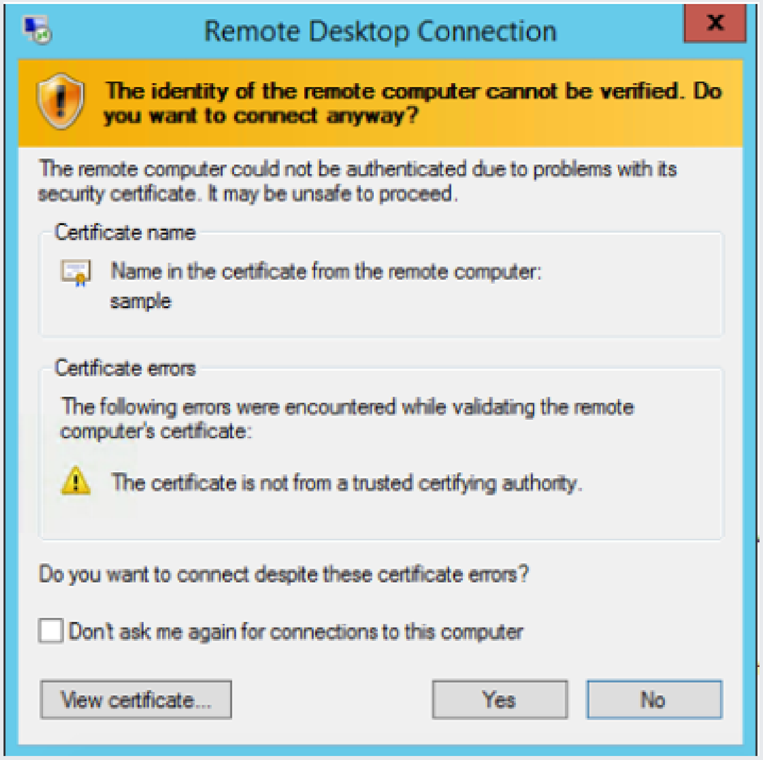
Type: Remote Desktop Connection

Remote computer: [redacted]

□ Don't ask me again for connections to this computer

This warning is due to the session being opened by creating a session file that is not signed because it is only used to start this session. The credentials used in the session file are encrypted.

Another warning might appear informing you that the identity of the remote computer cannot be identified.



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
sample

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

This warning appears because the connection is secured using a self-signed certificate, and, by default, your computer does not trust self-signed certificates. This certificate is not used to ensure the identity of the server but to secure the connection between your machine and the server.