Configuring Cisco UCS Director PowerShell Agent

This chapter contains the following sections:

Adding PowerShell Agent to Cisco UCS Director

After PowerShell Agent is installed and running, add it to Cisco UCS Director. Ensure to set up the virtual account (for example, an SCVMM account) to use the PowerShell Agent for inventory collection and other management functions.

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 On the **Virtual Accounts** page, click **PowerShell Agents**.

Step 3 Click **Add**.

Step 4 On the **Add Agent** screen, complete the following fields.

Name	Description
Agent name field	The name of the PowerShell Agent.
Agent Address field	The IP address or FQDN (Fully Qualified domain name) of the PowerShell Agent.
Agent Access Port field	The port assigned to the PowerShell Agent. **Note** The default port address is 43891. These values are pre-populated with default values. The PowerShell Agent is pre-configured to use these values and UCS Director must have matching values. These values can be changed on the Agent, but UCS Director must always use them as well.

Name	Description
Access key field	Enter access key of PowerShell Agent. You can do one of the following: • Use the existing authkey of PowerShell Agent. To get a copy of the authkey, see Copying authkey of PowerShell Agent. • Enter a new access key for PowerShell Agent. The alphanumeric and special characters are allowed. If you want to define a new access key, before entering the new key in Cisco UCS Director, update the value of access key as authkey in the PowerShell Agent `properties.xml` file available in the `%AGENT_INSTALL_FOLDER%/props/` path and restart the Cisco PowerShell agent service. After restart, wait for 15 seconds and then add new access key of PowerShell Agent to Cisco UCS Director. To restart the service in Windows machine: **a.** Enter **services.msc** in the **Run** box. **b.** In the **Services** screen, select **Cisco PowerShell agent service**. Right-click and select **Restart**. **Note** Only user with admin permission can edit the `properties.xml` file.
Description field	The description of the PowerShell Agent.

Step 5 Click **Submit**.

What to do next

Verify connectivity between Cisco UCS Director and the PowerShell Agent.

Verifying Connectivity with Cisco UCS Director

After the PowerShell Agent is added, you can check the connectivity between Cisco UCS Director and the PowerShell Agent.

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 On the **Virtual Accounts** page, click **PowerShell Agents**.

Step 3 From the **More Actions** drop-down list, choose **Test Connection**.

Cisco UCS Director displays a success message if it can communicate with the PowerShell Agent.

If Cisco UCS Director cannot communicate with the PowerShell Agent, see Troubleshooting Connectivity with Cisco UCS Director, on page 3.

What to do next

Execute the Cisco UCS Director PowerShell command.

Troubleshooting Connectivity with Cisco UCS Director

Problem

You can experience a failed test connection with Cisco UCS Director. This problem can occur even though you successfully installed and configured the PowerShell Agent, and there is no issue with the network connectivity between PowerShell Agent and Cisco UCS Director.

Note This problem can happen with Windows Server 2012 R2 or other versions that use advanced cipher suites for https communication.

Symptom

Check the PowerShell Agent log files in the PowerShell Agent server, for an **SSPI failed with inner exception** error. See sample error message:

```
2014-08-20 14:44:16,832 [6] ERROR cuic.ClientConnection[null] -
    Exception: A call to SSPI failed, see inner exception.
```

```
2014-08-2014:44:16,832 [6] DEBUG cuic.ClientConnection[null] - Inner exception:
The message received was unexpected or badly formatted.
```

```
2014-08-2014:44:16,832 [6] DEBUG cuic.ClientConnection[null] - Authentication
failed - closing the connection.
```

Cause

The test connection fails because of the Microsoft update, in which, new TLS cipher suites are added and cipher suite priorities are changed in Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2. See Microsoft kb article 2929281 for further information on this update.

Solution

To resolve the problem, modify the SSL cipher suite group policy setting. Follow the listed steps:

1. At a command prompt, enter `gpedit.msc` to open your group policy editor.

2. Expand **Computer Configuration** > **Administrative Templates** > **Network**, and then click **SSL Configuration Settings**.
3. Under **SSL Configuration Settings**, click the **SSL Cipher Suite Order** setting.
4. In the **SSL Cipher Suite Order** pane, scroll to the bottom of the pane.
5. Follow the instructions labeled **How to modify this setting**.

It is necessary to restart the computer after modifying this setting for the changes to take effect.

Authentication Mechanisms

After you have added the PowerShell Agent to Cisco UCS Director, you can set the authentication mechanism by creating a workflow with Execute PowerShell Command task.

The **Execute PowerShell Command Task** establishes a remote PowerShell session from PowerShell Agent to the target server to execute commands on that server. A **Default** authentication mechanism is currently used to set up the session. With this release, support is also extended to the following types of authentication mechanisms:

- **Basic Authentication**—Simple mechanism to transmit username and password to a web server or target machine in clear text.
- **Kerberos Authentication**—Mutual authentication process that uses encrypted keys between a client and a server machine. This protocol is selected to authenticate a domain account such that both the user identity and server identity are guaranteed without sending of any reusable credentials.
- **Negotiate Authentication**—Both the client and the server compute a session key from the user password without ever exchanging the password itself. It is selected for local computer accounts and is best suited for intranet web authentication.
- **Negotiate Authentication with Implicit Credentials**—Assigns an SSL certificate to a target server to guarantee both the user and the server identity. A client trusted Certificate Authority issues the SSL certificate.
- **CredSSP Authentication**—Intended for environments where Kerberos delegation cannot be used. To use CredSSP authentication, delegate the PowerShell Agent as a CredSSP client for the target machine.

Note Multi-hop support in Windows Remote Management (WinRM) uses CredSSP for authentication. Since PowerShell is built on top of WinRM, you can use CredSSP to perform multi-hop authentication.

When you add a new workflow for the Execute PowerShell Command Task, one of the input fields is **Authentication Mechanism**. It provides you an option to choose the type of authentication you wish to set-up for the remote session.

For detailed steps on how to execute the task and set your authentication between the PowerShell Agent and target server, see Executing PowerShell Commands.