Saviynt – Active Directory (ADSI) Integration & Design Document

February 2023

Table of Contents

[Introduction 3](#_Toc126762963)

[Supported Features 4](#_Toc126762964)

[Supported Version 4](#_Toc126762965)

[Server Specifications 5](#_Toc126762966)

[Prerequisites 5](#_Toc126762967)

[Installing IIS 6](#_Toc126762968)

[Installing the ADSI Agent 8](#_Toc126762969)

[Moving an Object Between Domains in the Same Forest 11](#_Toc126762970)

[Invoking PowerShell Script Through Saviynt 12](#_Toc126762971)

[Configure Windows Server to Execute PowerShell Scripts 12](#_Toc126762972)

[Installation of Windows Internet Information Services Server 13](#_Toc126762973)

[Deploying Saviynt App on Windows Server 20](#_Toc126762974)

[Deploying PowerShell Script on Windows Server 23](#_Toc126762975)

[Rest Connector 23](#_Toc126762976)

[Active Directory Password Policy 23](#_Toc126762977)

[ADSI Connector Design 24](#_Toc126762978)

[Create Account via Saviynt Technical Rules 24](#_Toc126762979)

[Add Access 25](#_Toc126762980)

[Remove Access 26](#_Toc126762981)

[Reconciliation 27](#_Toc126762982)

[Account Enable 29](#_Toc126762983)

[Account Disable 30](#_Toc126762984)

[Account Removal 31](#_Toc126762985)

Document Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version control** | | | |
| **Version** | **Name** | **Role** | **Date** |
| v1 | Shuangyue Wu | Author | 01/30/2023 |
| v2 | Gaurav Khandelwal | Author | 02/01/2023 |
| v3 | Vineet Gupta | Author | 02/08/2023 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision history** | | | | |
| **Version** | **Changed Sections** | **Details of Change** | **Date** | **Changed By** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Introduction

**Saviynt Active Directory Service Interfaces (ADSI)** **connector** provides ability to create an integration with Active Directory and perform operations on user and group objects located in multiple domains in a single or multiple forests. The connector simplifies the overall deployment and integration of forests with the Saviynt Identity Governance solution.

Active Directory Service Interfaces (ADSI) is a set of component object model interfaces provided by Microsoft for accessing the features of Active Directory services. The connector leverages the ADSI LDAP protocol to query and manipulate Active Directory objects and automate common tasks. These tasks include adding users and groups, managing service accounts, and setting permissions on users, accounts, and groups.

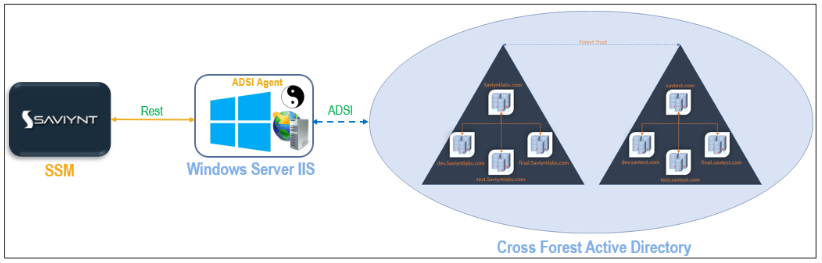


Figure 1: Architecture diagram of ADSI Connector

1. The ADSI connector deployed on SSM (Saviynt Security Manager) establishes communication with the ADSI agent deployed on the target application or a member server using REST APIs.
2. The ADSI agent request to domain controller or the cross-forest setup using ADSI’s LDAP protocol.
3. The ADSI agent returns the result (information) to SSM.

Supported Features

The Saviynt ADSI connector supports the following features:

|  |  |  |
| --- | --- | --- |
| **Feature** | **Supported Operation** | **Description** |
| **Reconciliation** | User Management (import users) | Supports full or incremental import of users to SSM. |
| Account Management (import accounts) | Supports full or incremental import of accounts to SSM after the users are available in SSM. SSM uses the User Account Correlation rule to map accounts with users. |
| Access Management (import access) | Supports full or incremental import of entitlements to SSM along with the accounts that have access to those entitlements. This operation also supports a single or nested group import. |
| **Provisioning** | Account Management | Supports the following provisioning operations:   * Create or update account information * Add or remove access * Enable, disable, and delete accounts |
| Service Account Management | Supports provisioning operations such as create, update, and delete service accounts. |

Supported Version

Active Directory 2016 and later.

Server Specifications

|  |  |
| --- | --- |
| Specifications | Value |
| CPU | 4 Core 64-bit processor |
| RAM | 15 GB |
| Storage | 100 GB |

**Ensure that the following software is installed:**

* .Net Framework 4
* Windows Internet Information Services (IIS) Server
  + Windows Server 2012 R2 or later
  + IIS Version 7 or later

Prerequisites

**Following are the tasks required to be completed before starting integration with Saviynt:**

* Internet Information Services (IIS) is installed on the host operating system where Active Directory is installed, or a member server that belongs to a domain but is not the domain controller, or a domain in a forest.
* ASP.NET 3.5 and 4.6 roles are installed on the server where IIS is installed.
* ADSI Agent (C# based agent) is deployed on the domain or on the member server where IIS is installed.
* Logged in user on this windows machine will need Domain Administrator rights to perform the requested tasks on user and group objects in the target application.
* It is recommended that this machine belong to domain as that of the Parent instead any of the child domain.
* Forest-level trust is configured when objects belong to different forests.
* **(Optional)** The target object (user/contact) is moved within or outside a domain. For example, a user account is moved from one Organization Unit to another when the user is transferred from one department to another in your organization. This enables the user to receive the benefits and restrictions defined for the new Organization Unit.
  + Movement of an object within a domain is internally handled by the Move ADSI API.
  + Movement of an object across domains in the same forest is handled by the Movetree utility. This utility must be installed on the primary domain server.

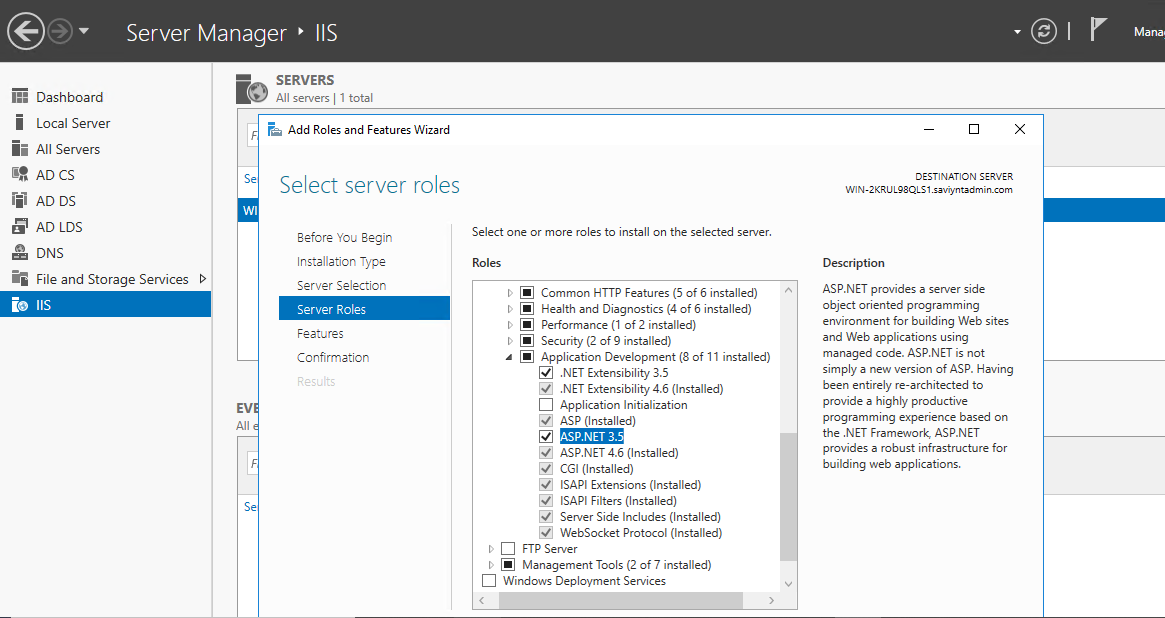
The trusts between domains in a forest are transitive and two-way. Trust between domains of different forests must be created if we need to allow users from one domain to access resources in another domain in a different forest.

Installing IIS

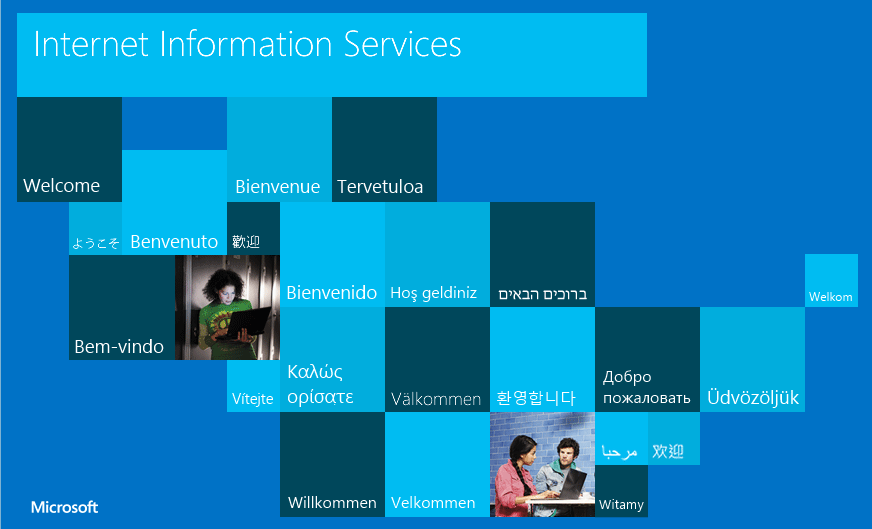
You can install IIS in two ways: GUI or Windows PowerShell command-line interface (CLI). If you do not have the GUI installed, use the PowerShell method. This method is relatively faster than the GUI method. For usage instructions, visit the [Microsoft Documentation](https://docs.microsoft.com/en-us/windows/) web site and search for the instructions for your operating system.

This section provides a detailed procedure for installing IIS web server version 10.0 on Windows Server 2016. For installing IIS on other supported Windows Server versions, see the corresponding instructions in the [Microsoft Documentation](https://docs.microsoft.com/en-us/windows/).

1. Click the **Start** icon.
2. Open **Server Manager**. Alternatively, search for it from the **Start** menu.
3. Click **Add roles and features**.
4. Before you begin the window, click **Next**. Select Programs and Features.
5. In the Select installation type window, leave **Role-based or feature-based installation** selected and click **Next**.
6. If you are installing IIS on a local machine, leave **Select a server from the server pool** with the current machine selected and click **Next**. Alternatively, select another server to install it.
   * From the Select server roles window that opens, select **Web Server (IIS)**. If this action opens a new window prompting you to add the required additional features, click **Add Features** to install these features, then click **Next** on the Select server roles menu.
   * If you do not want to install any additional features, click **Next** in the Select features window.
7. Click **Next** on the Web Server Role (IIS) window after reading the information provided.



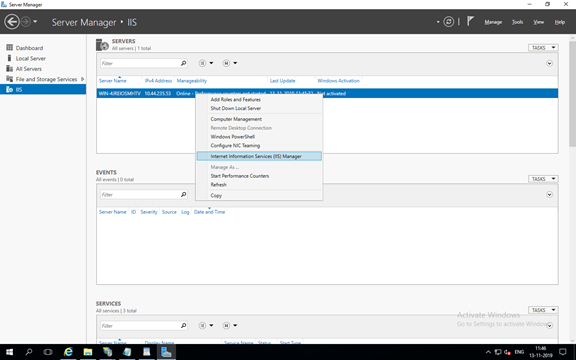
1. Click **Next** to install the defaults.
2. In the Confirm installation selections window, review the items for installation and click **Install**. A standard IIS installation does not need a system reboot unless the role is removed.
3. If the installation is successful, click **Close**. By default, IIS runs on port 80 with the firewall rule “World Wide Web Services (HTTP Traffic-In)” automatically enabled in the Windows firewall.
4. To verify if IIS is properly installed, open a web browser and browse to the server on which you installed IIS. It must open the default IIS page as below.

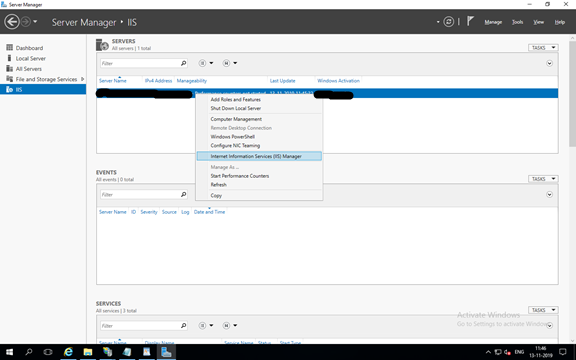


Installing the ADSI Agent

This section provides a detailed procedure for installing the ADSI agent on Windows Server 2016. The steps might vary for installing it on other supported Windows Server versions.

1. Log in to the computer where IIS is installed.
2. Open **Server Manager** > **IIS**, right-click the server name and open **Internet Information Server (IIS) Manager**.

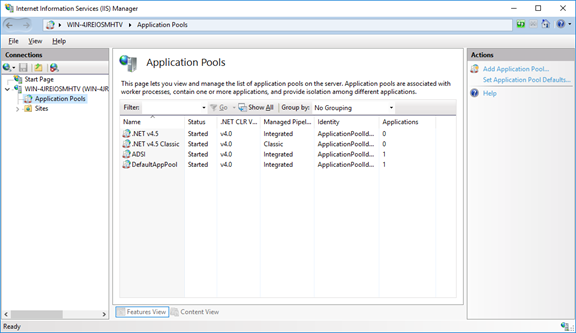




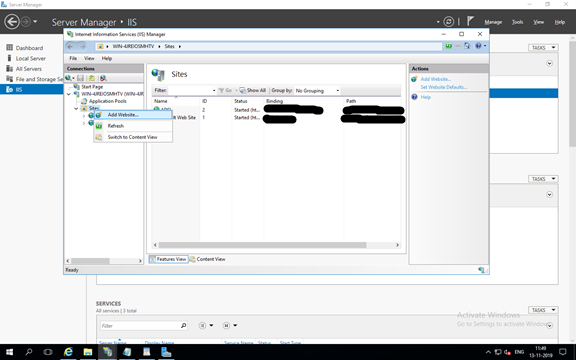
1. After IIS Manager is launched, manually install the ADSI agent binaries on the target computer.
   1. Open Internet Information Server (IIS) Manager.
   2. Click **+** to open the tree view of the server.
   3. Choose **Application Pool**.
   4. From the menu, click **Action > New >** **Application Pool**.
   5. In the **Add Application Pool** dialog box, enter the following details and click **OK**:  
      Name of the application pool.

The .NET Framework version your site or application uses.

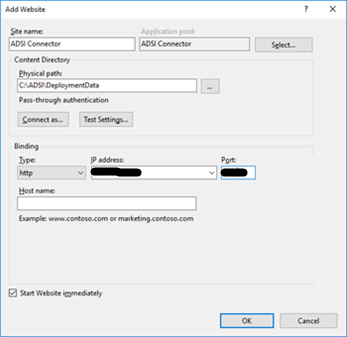
Integrated as the managed pipeline mode to allow your HttpModules to participate in all requests, including those for static content, PHP pages, and images.



* 1. Right-click **Sites**and select**Add Website**.



* 1. Specify the Site Name, Physical path (path pointing to deployment package), select the IP address in the binding option (IP address of the server where IIS is installed), provide the port which is not in use by other websites and click **OK**.



* 1. To install the SSL certificate for this website, see [Installation of SSL/TLS Certificate In Microsoft IIS 7](https://support.microsoft.com/en-in/help/324069/how-to-set-up-an-https-service-in-iis).

Moving an Object Between Domains in the Same Forest

Active Directory allows you to move objects (user objects scoped for this connector) between domains in the same forest using the Movetree command-line utility. You must install the utility on your primary domain server. If the utility is not available in your Forest on a primary domain, download it for your Windows version from the [Microsoft Support site](https://www.microsoft.com/en-in/download/details.aspx?id=15326). It is available as part of the Active Directory Support Tools installation package. Before running the Active Directory Support Tools installation program, ensure that all the previous versions of Microsoft Windows support tools are removed from your computer including the beta versions. If your computer has an older version of a support tool, you can instruct the installation program to automatically uninstall it or choose to uninstall it manually.

1. Download and extract the contents of the Active Directory Support Tools package.
2. Browse to the folder containing the suptools.msi program.
3. Run suptools.msi as an administrator.
4. In the Wizard that appears, do not change the default settings and complete the installation.

The wizard places the support tools including the Movetree utility in the C:\Program Files\Support Tools folder and creates an entry in the Windows registry.

Invoking PowerShell Script Through Saviynt

### Configure Windows Server to Execute PowerShell Scripts

Saviynt Security Manager (SSM) communicates to Windows Server through an application, namely, SaviyntApp, an application developed by Saviynt and is provided by Saviynt support for each client via the support channel. The SaviyntApp invokes a PowerShell (PS) session on the Windows Server and executes PS scripts.

Following version of components need to be installed on Window server so that Saviynt connector communicates with Windows agent and invoke PowerShell script.

* .Net Framework 4
* Windows Internet Information Services (IIS) Server
  + Windows Server 2012 R2 or later
  + IIS Version 7 or later
* SaviyntApp or Saviynt PowerShell Agent Package

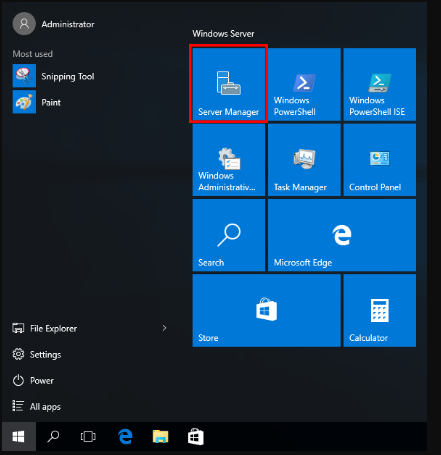
You must have the login credentials with administrator rights for hosting Windows Server and the ability to execute desired PowerShell scripts/commands.

### Installation of Windows Internet Information Services Server

This section provides information about the installation of Internet Information Services Server (IIS) on an intermediary server which is Windows Server. To install IIS Server from the Windows Server User Interface, perform the following steps:

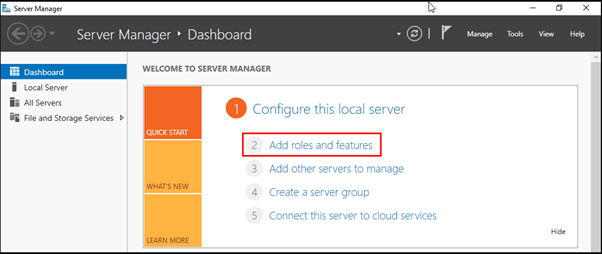
1. Open Server Manager from Start menu. Type “Server Manager” from the search bar near the Start menu to open the Server Manager.

Figure 1: Selecting Server Manager option

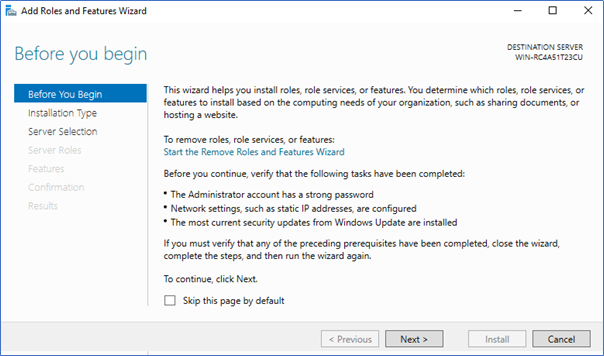


1. In the Server Manager Dashboard, click Add roles and features.

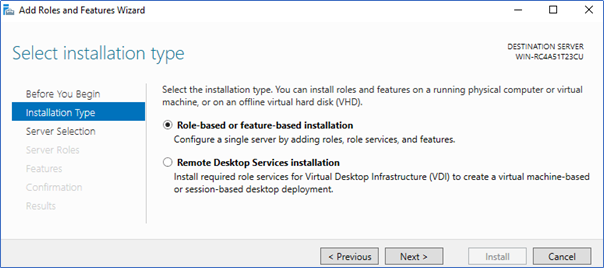
Figure 2: The Add Roles and Features Wizard



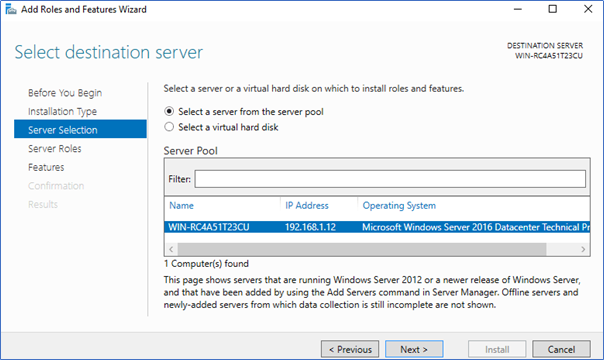
1. In the “Before You Begin” window, click Next button.

Figure 3: Before You Begin Window in Add Roles and Features Wizard

1. In the Select installation type window, check Role-based or feature-based installation, and click Next.

Figure 4: Select Installation Type Window

1. Check Select a server from the server pool with the current Windows Server selected and click Next.

Figure 5: Selecting the Destination Server

The Select server roles window is displayed.

1. From the Select server roles window, check Web Server (IIS) option.

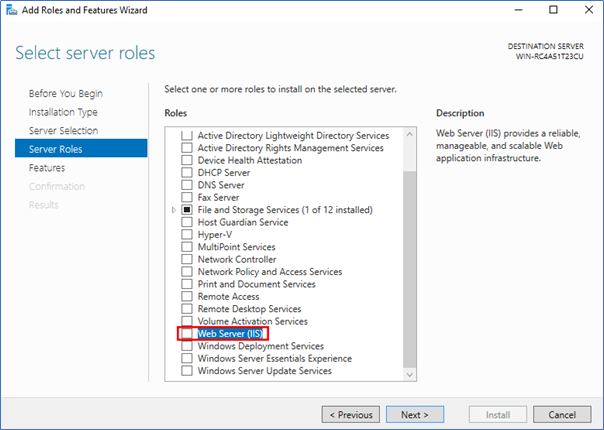
Figure 6: Selecting Server Roles  


Figure 7: Select Server Roles Continued

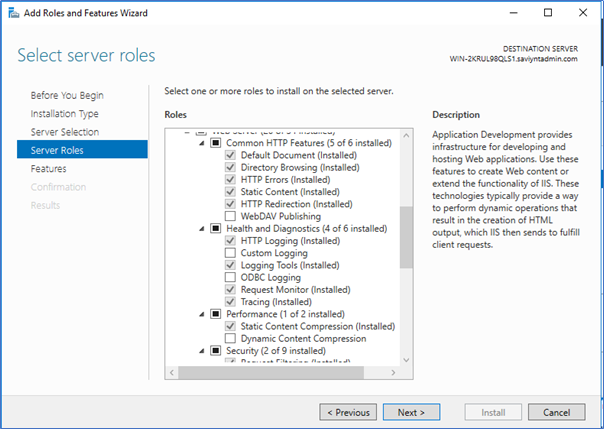


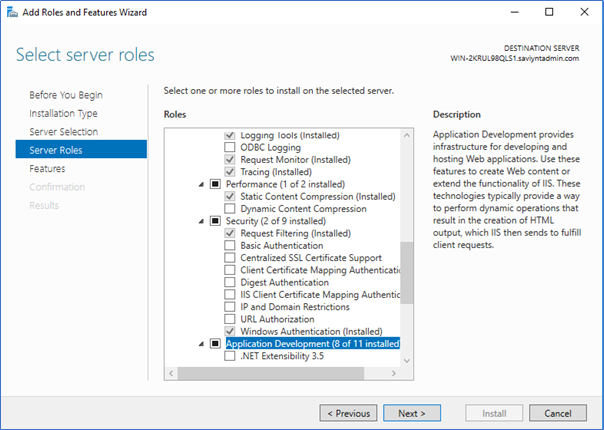
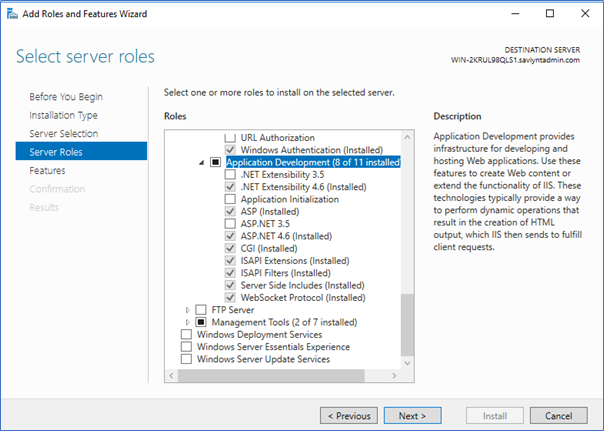
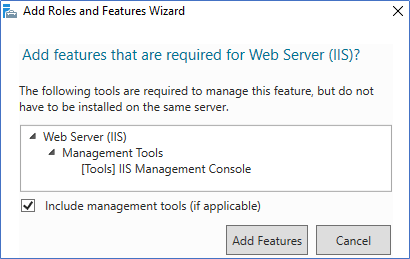
Figure 8: Select Server Roles Continued

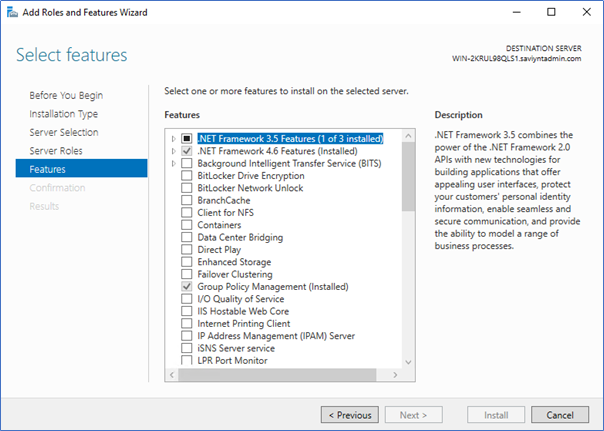
Figure 9: Select Server Roles Continued

1. Click Next. A new window is displayed with the message that additional features are required.
2. Click Add Features to install the additional features.

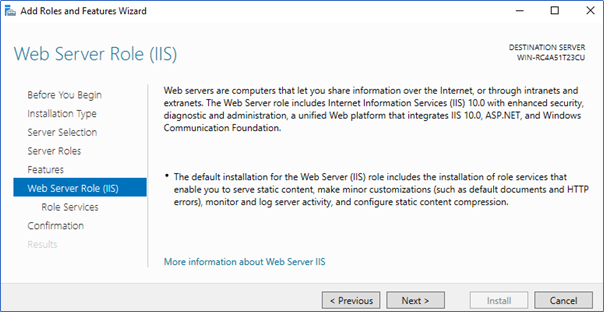
Figure 10: Add Features Option



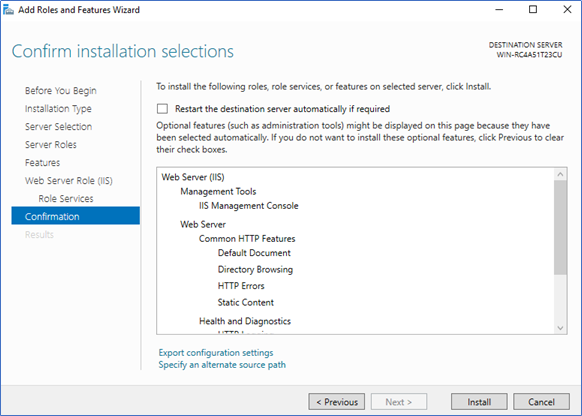
1. At this stage, no additional features are installed; hence click Next on the Select features window.

Figure 11: Select Features Window

1. Click Next in Web Server Role (IIS) window based on the information (text) provided about Web Server (IIS) role in the window.

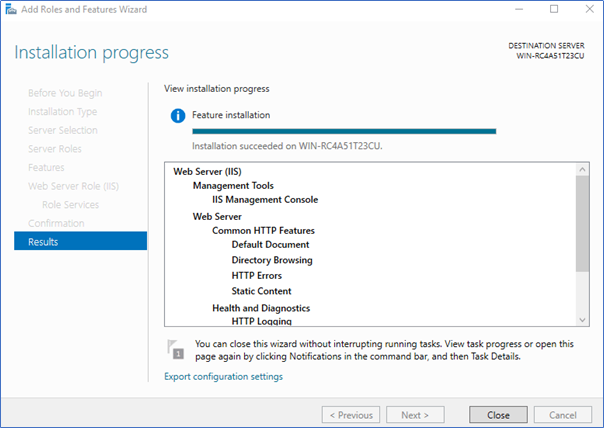
Figure 12: Web Server Role (IIS)

1. At this point, in the Select role services, you can install additional services for IIS.
2. In the Confirm installation selections window, review the items to be installed and click Install. This installs the IIS web server.

Figure 13: Confirming Installation Selections  


A reboot is not required in a standard IIS server installation; however, if you remove the role, a reboot is required.

1. After the installation is completed, click Close.

Figure 14: Installation Progress and Completion 

IIS is installed and runs on port 80 (by default) with the firewall rule World Wide Web Services (HTTP Traffic-In) automatically enabled in the Windows firewall.

After this installation is completed, install the SaviyntApp.

### Deploying Saviynt App on Windows Server

Use the following link to download the Saviynt App (or “Saviynt PowerShell Agent”) to your system:

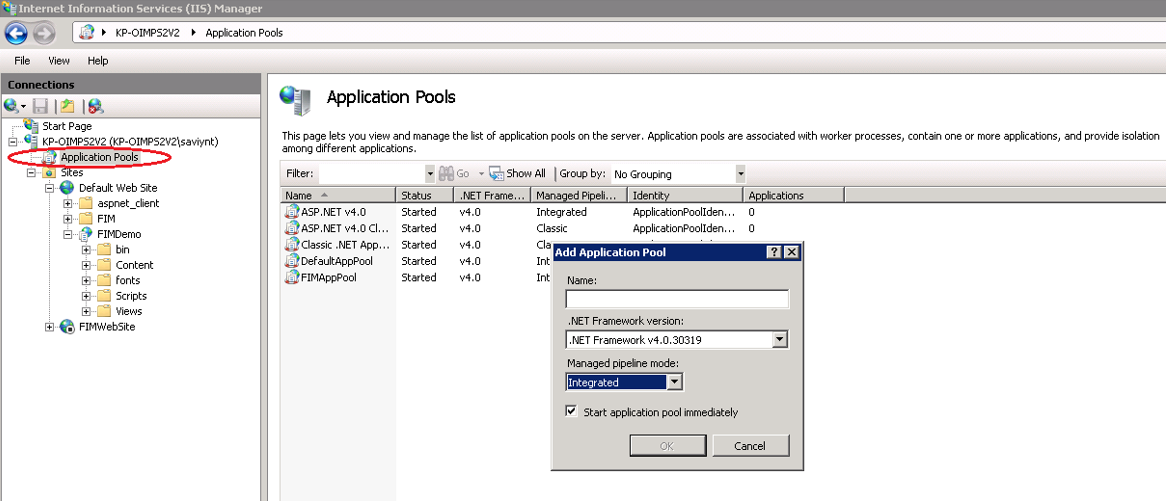
Table 3: Download Saviynt PowerShell Agent

|  |  |
| --- | --- |
| Saviynt PowerShell Agent | |
| URL | https:// SAVIYNTAWSURL/Saviynt-Powershell/Saviynt-PowershellAgent.zip (Provided by Saviynt support team) |

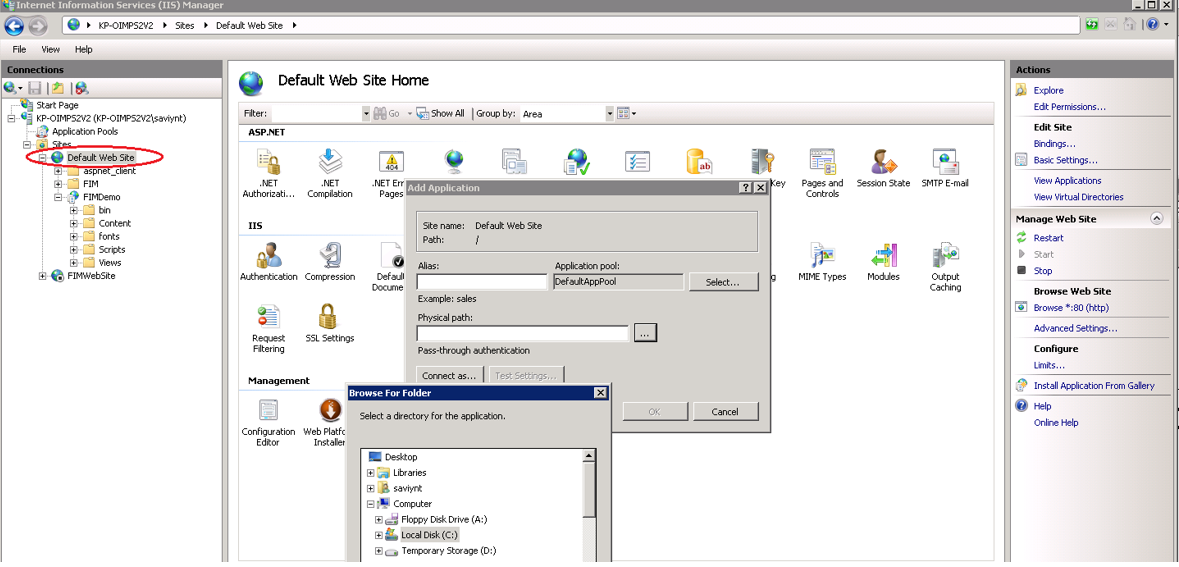
**Please note:** SAVIYNTAWSURL – will be provided by Saviynt support team

To deploy Saviynt App in the Windows IIS Server, perform the following steps:

1. Add an application pool with .Net Framework 4 version.
   1. In the IIS Manager, create an application pool and provide a name.
   2. Select .net framework4 and mode as integrated and click **OK**.

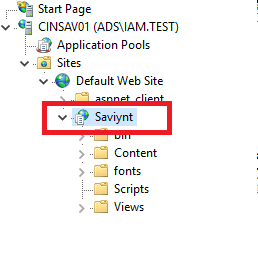
Figure 15: Adding Application Pool

1. Create an application under Default Web Site.
   1. Provide a name in the Alias field.
   2. Select the app pool created in Step1 for the Application pool field.
   3. For the physical path, select the local folder path where you plan to deploy the code, for example, C:\inetpub\wwwroot\SaviyntApp. You can create new folders in the "Browse for" folder window.

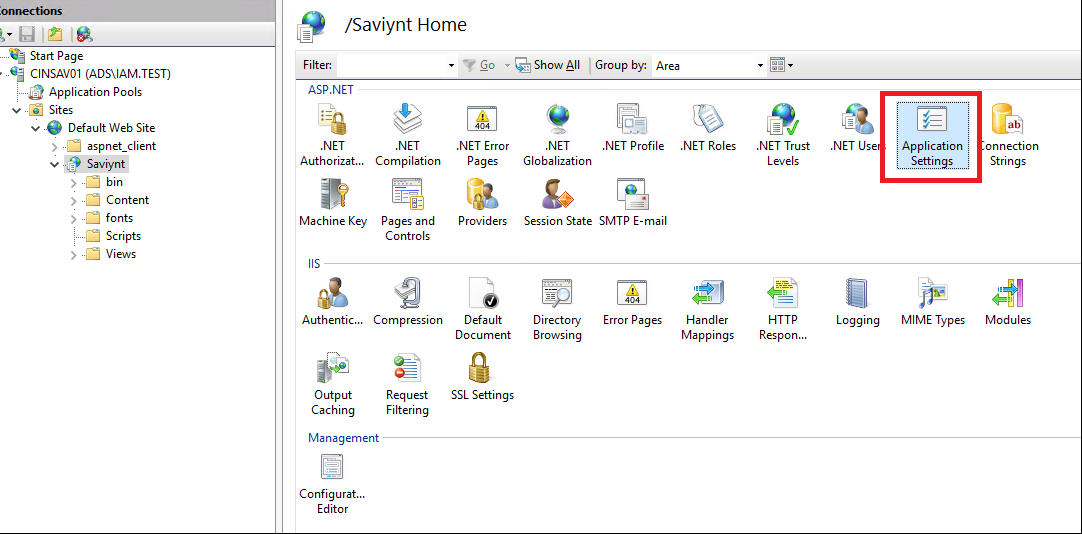
Figure 16: Creating an Application within the Default Web Site

1. Copy the Saviynt App package in the physical path mentioned in Step 2.
2. Navigate to Saviynt as shown below and click on Saviynt.

Figure 17: SaviyntApp

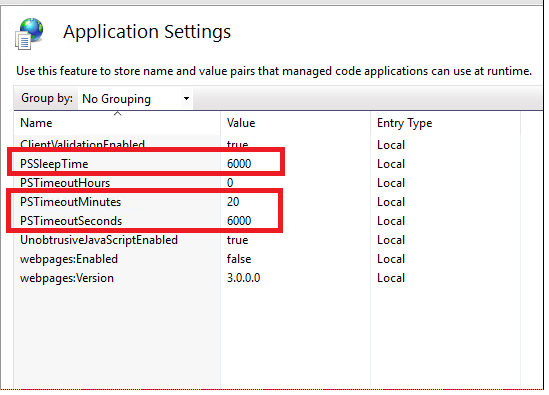


1. Search for Application Setting and double click on Application Setting.

Figure 17: SaviyntApp Application Setting

1. Change the value for PSSleepTime=6000, PSTimeoutHours=20 and PSTimeoutSeconds=6000

Figure 19: Application Setting



### Deploying PowerShell Script on Windows Server

To deploy **PowerShell Script** in the Windows IIS Server, perform the following steps.

1. Copy following PowerShellScript.zip into C:\ drive on Windows ISS Server <AD Server> and unzip PowerShellScript.zip file.

Rest Connector

For executing PowerShell scripts, we either need a REST or Windows connector. Hence, we need to create a Rest Connection, a security system and an Endpoint.

#### Create Connection in Saviynt

1. Login to SSM with administrator user credential.
2. Click on “Admin” on the top right corner and then on “Identity Repository”. Under the “Identity Repository” select “Connections”.
3. Click on “Actions” and then “Create Connections”.
4. Fill the details of the connections as per details provided in deployment document.

Active Directory Password Policy

Below is the table for defining a sample AD Password Policy in Saviynt.

|  |  |
| --- | --- |
| **Attribute Name** | **Attribute Value** |
| Policy Name | **Active Directory Password Policy** |
| Policy Description | Active Directory Password Policy |
| Policy Scope | Application |
| Maximum Repeated Characters | 2 |
| Minimum Numeric Characters | 1 |
| Minimum Special Character | 1 |
| Minimum Alphabet Characters | 1 |
| Use Blacklist Dictionary | NO |
| Minimum Length | 8 |

Active Directory Use Cases

### Create Account via Saviynt Technical Rules

When a Saviynt user is created or updated via HR System, technical rule can be be triggered to provision user in Active Directory.

### Add Access

This is the flow to provision Active Directory entitlements/groups to company employees and contractors as a request from the Saviynt.



* + 1. Launch the ARS. User can request entitlement for others or for self.
    2. Select AD Endpoint and modify which will redirect to account modification page.
    3. Select the groups that needs to be added and submit the request.
    4. Once request approved, it will create pending tasks. If no approval workflow is defined, requests are auto approved.
    5. Run the WSRETRY Provisioning job to complete the pending task and add the group membership to the user in Active Directory.

### Remove Access

This is the flow to de-provision Active Directory entitlements/groups from company’s employees and contractors as a request from the Saviynt.



* + 1. Launch the ARS. User can request to remove group for others or for self.
    2. Select AD endpoint” and modify which will redirect to account modification page.
    3. Select the groups that needs to be removed and submit the request.
    4. Once request approved, it will create pending tasks. If no approval workflow is defined, requests are auto approved.
    5. Run the WSRETRY Provisioning job to complete the pending task and remove the group membership from the user in Active Directory.

### Reconciliation

Account reconciliation will be configured for Active Directory. This process will make Saviynt aware of the existing Active Directory account and in sync with Active Directory.



1. It will bring the account if not exists and correlate it to user if correlation rule matched.
2. If account exists, then update the existing account fields in SSM instead of creating new one.
3. Set the status of account to In-active/Active in SSM for all disabled/enabled AD users coming through reconciliation process based on the value “useraccountcontrol”.
4. There are two types of reconciliation Account reconciliation, which will bring only accounts and Access Reconciliation, which brings groups along with its members.

Group reconciliation will be configured for Active Directory. This process will make Saviynt aware of the existing Active Directory group and in sync with Active Directory.



1. It will bring the group along with its members if not exists.
2. If group exists, then update the existing group fields along with its members in SSM.

**Account Reconciliation Jobs:**

|  |  |
| --- | --- |
| Job Name | Purpose |
| ACTIVEDIRECTORY \_FULL\_ACCOUNT\_RECON | It will bring full set of active directory users into Saviynt to make in sync. |
| ACTIVEDIRECTORY \_INCREMENTAL\_ACCOUNT\_RECON | It will bring recently created or updated users after last run. |

**Access Reconciliation Jobs:**

|  |  |
| --- | --- |
| Job Name | Purpose |
| ACTIVEDIRECTORY \_FULL\_ENTITLEMENT\_RECON | It will bring full set of active directory groups along with its members into Saviynt to make in sync. |
| ACTIVEDIRECTORY \_INCREMENTAL\_ENTITLEMENT\_RECON | It will bring recently created or updated groups along with its members after last run. |

### Account Enable

When a user is rehired within X days of leave or returning from long term LOA, Active Directory Provisioning can be triggered via rules to enable account.



1. If the Deleted flag is enabled and user is in active state, it indicates user is rehired after X days of termination.
2. The Employee Job Status should be updated to “A” for returning long term LOA user and his/her Disabled Date field should be null.
3. The user update rules will trigger Active Directory provisioning to enable account.

### Account Disable

When a user is terminated or taking long term LOA, Active Directory Provisioning will be triggered to disable account.



1. If Status is updated to 0, Network Access is N and Employee Job Status is changed to L/P, it indicates that the user is taking long term LOA.
2. If Employee Job Status is updated to T/U/D/Y and Emergency Terminated is Null or No, it indicated the user is terminated from HR source.
3. The user update rule will trigger Active Directory provisioning to disable account.
4. If user is terminated, Saviynt will set Termination Date for user as well.

### Account Removal

When a user is terminated and the Disable Date is prior X days of current date, Active Directory Provisioning will be triggered to delete account.



1. There is a logic to calculate the difference between Disable Date and current date.
2. If a user is terminated more than X days, Deleted Status will be set to Deleted.
3. Active Directory de-provisioning will be triggered to delete account.