Okta Identity Cloud for ServiceNow

Configuring the Okta Application from the ServiceNow App Store

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

Table of Contents

What is the Okta Identity Cloud for ServiceNow application?

The Okta Identity Cloud for ServiceNow Application (OIC app) is the simplest way to get ServiceNow connected to Active Directory (AD) and provide provisioning, de-provisioning, and Single Sign-On (SSO) services via Okta for ServiceNow.

This new integration allows for two major performance enhancements:

1. Provisioning of user accounts into ServiceNow to include any standard attribute in the sys_user table, as well as any custom attributes that may have been added by the ServiceNow administrator

2. Full support of the current ServiceNow API set, ensuring that any future capabilities can be supported by Okta.

How do I get the Okta Identity Cloud for ServiceNow app?

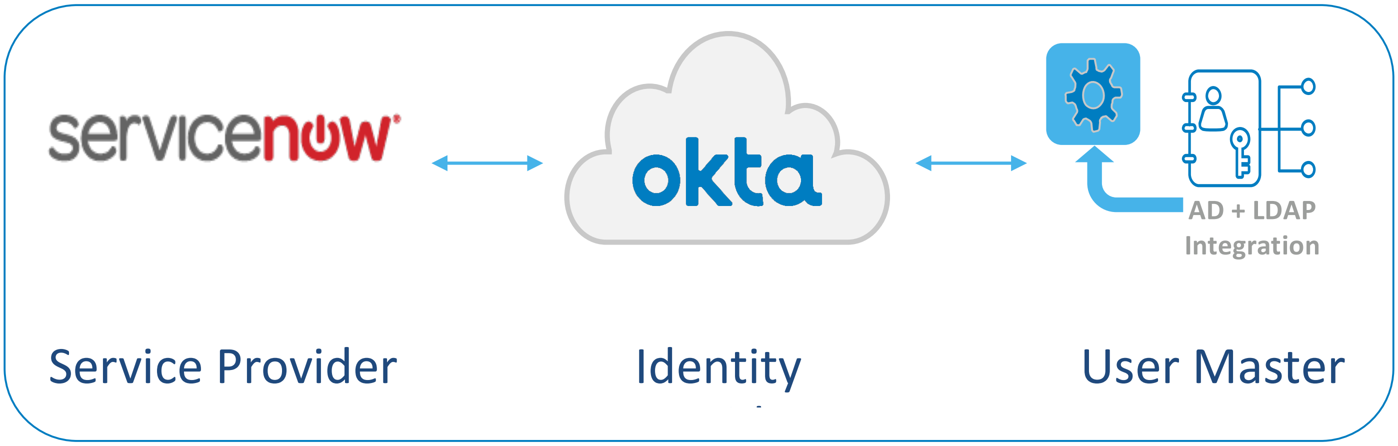
The Okta Identity Cloud for ServiceNow Application (OIC app) is available in both the ServiceNow Express and ServiceNow Enterprise Stores.

The application supports ServiceNow instances on Helsinki and newer versions, and in these cases, the older 'SSO Provided By Okta' plugin should no longer be used.

How do I connect ServiceNow and Okta?

Connect ServiceNow and Okta by way of the OIC application in ServiceNow, then connect Okta and Active Directory by way of the Okta Active Directory Agent.

FIGURE 1: Architectural Overview



This Deployment Guide is applicable to the Okta Identity Cloud for ServiceNow application, which is available in the Store for ServiceNow Express and ServiceNow Enterprise.

The sections that follow provide a more detailed installation checklist and specific instructions on each configuration item.

Configuration checklist

Use this configuration checklist to help you install and configure both ServiceNow and Okta to enable single sign-on and user provisioning from Okta to ServiceNow. Also, we highly recommend that you see Appendix A for general Okta best practices that apply to all Okta scenarios.

Step		Page #
1	Download the Okta Identity Cloud for ServiceNow application from the ServiceNow store.	on page 3
2	Configure the Okta Identity Cloud for ServiceNow application in ServiceNow: • Validate that Okta org is automatically created (if applicable). • Validate that ServiceNow UD app is automatically created in Okta.	on page 3
3	Install and configure the Okta Active Directory agent on a domain-joined server.	on page 7
4	Import users and groups from AD to Okta.	on page 8
5	Enable provisioning features in Okta for ServiceNow. • Decide on user attributes to push to ServiceNow from Okta.	on page 8
6	Determine user and group assignment plan. • Test and verify SSO and provisioning for AD-mastered User. • Choose groups for user management.	on page 11
7	Enable Desktop SSO (Windows Integrated Windows Authentication (IWA) server). (optional)	on page 14
8	Set up High Availability (HA) for AD agent and IWA server.	on page 14
9	Enable Password Reset. (optional)	on page 15

1 Download the Okta Identity Cloud for ServiceNow Application

Follow the standard ServiceNow store download procedure to install the Okta Identity Cloud for ServiceNow application into your ServiceNow instance. Once the application is available and installed, you will see the Okta Identity Cloud for ServiceNow application in the left-side navigation bar, and the configuration page will be available.

2 Configure the Okta Identity Cloud for ServiceNow app

Configuration steps inside of the OIC app are identical for ServiceNow Enterprise and ServiceNow Express. Post-configuration steps differ slightly, and section 2.1.3 covers the differences.

Note: If you are an existing Okta customer and have an Okta org that you'd like to use, please see Section 2.3.2.

2.1 Configuring the app without an existing Okta org

Note: This section assumes that there is no current Okta org available and will let the Okta application automatically create one.

The Okta Identity Cloud for ServiceNow application configuration page provides Okta with all the information needed to create an Okta org and configure the ServiceNow integration for single sign-on.

To configure the application, follow these steps:

1. Select *Okta Single Sign-on > Provider Setup* in the left index in ServiceNow

2. Uncheck the *Existing Customer* radio button.

3. In the *Okta Prefix* field, enter the desired subdomain name for your Okta org. For example, enter 'MyCompany' to claim 'mycompany.okta.com.'

   This company name must be unique; the application will show an error if you choose a name that is already in use. Simply choose another name for the subdomain.

4. In the *Company Name* field, enter your actual company name.

   This field must be unique to Okta, so if you have previously created a Sandbox or Trial instance of Okta, you may need to provide a custom suffix to your company name (ex. My Company 2).

5. In the *Administrator First Name* field, enter the administrator's first name. Please do not use a service account or alias name here.

6. In the *Administrator Last Name* field, enter the administrator's last name.

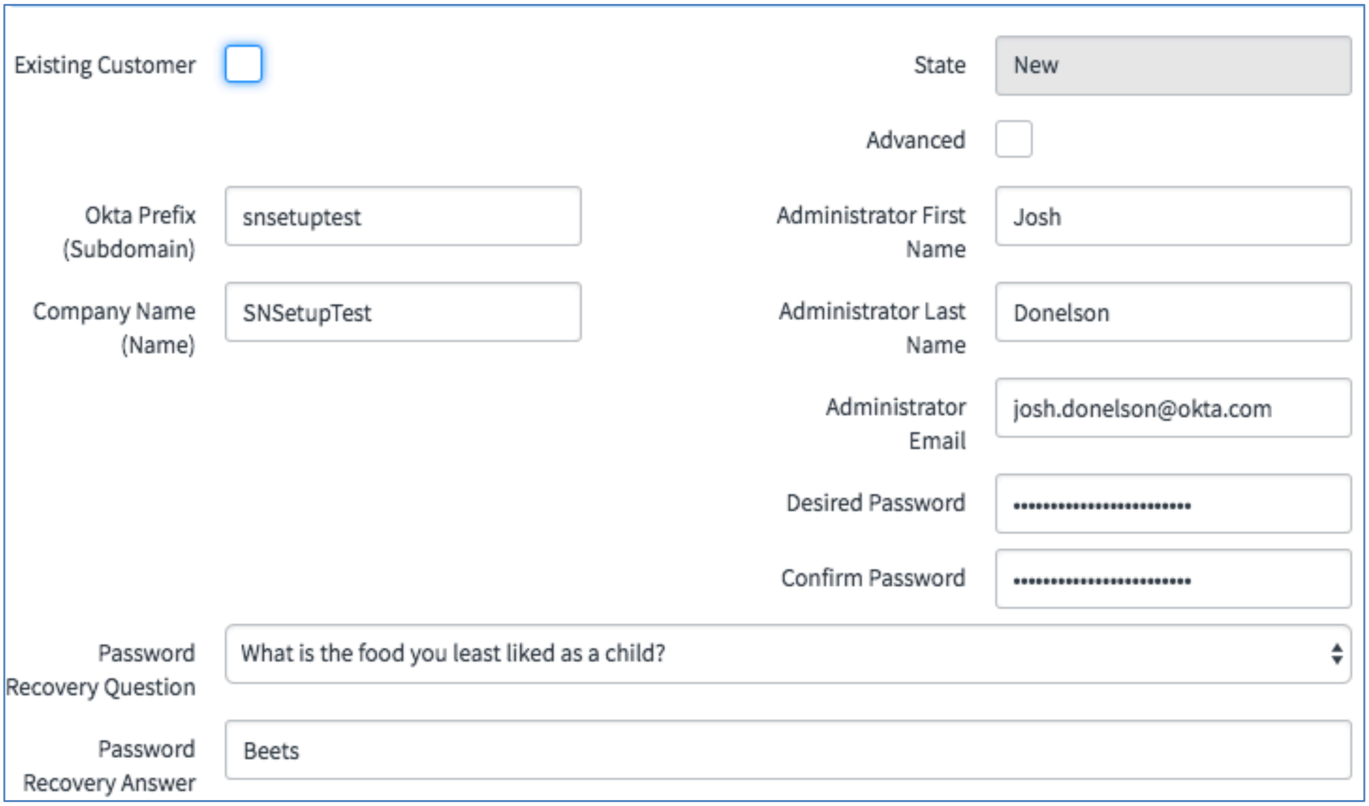
7. In the *Administrator User Name* field, enter the email for the administrator. Please use a valid company email address, as this email is used for Okta communications.

   This email address will also be the username of the first administrator on your Okta org.

8. In the *Desired Password* field, enter the starting password for the Okta administrator. Confirm the password. You can change this later.

9. Select a password recovery question, and enter an answer.

10. If you need to return to the setup form at a later date, you can save the current state by clicking the Save Setup button. Otherwise, click Provision to complete and create your Okta instance.



Existing Customer □

State: New

Advanced □

Okta Prefix (Subdomain): snsetuptest

Company Name (Name): SNSetupTest

Administrator First Name: Josh

Administrator Last Name: Donelson

Administrator Email: josh.donelson@okta.com

Desired Password: ••••••••••••••••••••••••

Confirm Password: ••••••••••••••••••••••••

Password Recovery Question: What is the food you least liked as a child?

Password Recovery Answer: Beets

If configured successfully, you will see the following occur:

- Details about your new Okta org appear on the reloaded page
- You can link directly to the IdP Record created in ServiceNow to support authentication from this Okta org.
- Checking the *Advanced* radio button shows additional information about your Okta org (this information is read-only).

2.2 Configuring the app with an existing Okta org

Note: This section applies to customers who are already Okta customers. If you completed Section 2.3.1, skip this section and proceed to 2.3.3.

The steps in this section automatically configure the ServiceNow application inside of the existing Okta org. You *do not need* to manually add the application inside of the Okta org.

First, obtain a valid API key from the Okta instance.

1. Log into Okta as an administrator. Please ensure the user obtaining the key is a Super-Admin; the ServiceNow auto-configuration process requires Super-Admin API access.

2. Obtain this API key by a User Account that will not be deactivated. The API key generated is tied to the user account and current user password, and it will be revoked by the system if that user information changes. We recommend using an administrative Service Account in Okta.

3. Under Security > API, choose **Create Token**.

4. You will have only one chance to see the key, so copy the text to a secure location.

Next, to configure the application, follow these steps:

The Okta Identity Cloud for ServiceNow application configuration screen in ServiceNow provides Okta with all the information needed to fully configure the ServiceNow integration for single sign-on.

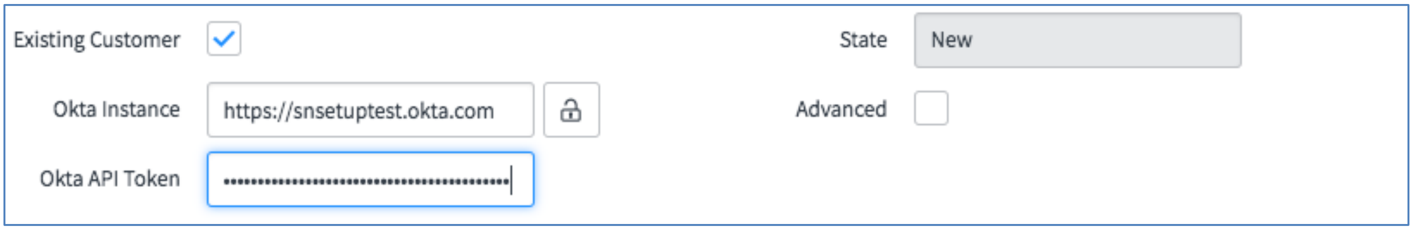
1. Select *Okta Single Sign-on > Provider Setup* in the left index in ServiceNow

1. Click the *Lock Icon* next to the *Okta Instance* field to open that field for editing. Enter the full URL of your Okta instance, including the HTTPS:// prefix.

2. In the Okta API Token field, paste the API that you generated from Okta.

3. If you need to return to the setup form at a later date, you can save the current state by clicking the Save Setup button. Otherwise, click Provision to complete the setup.

Figure 3: Existing Okta tenant configuration parameters



Existing Customer ☑

State: New

Okta Instance: https://snsetuptest.okta.com

Advanced □

Okta API Token: ••

If configured successfully, you will see the following occur:

- Details about your new Okta org appear on the reloaded page

- You can link directly to the IdP Record created in ServiceNow to support authentication from this Okta org.

- Checking the *Advanced* radio button shows additional information about your Okta org (this information is read-only).

2.3 Post-configuration steps

1. Browse to the Okta org you specified during setup, and log in using the administrator username and password.
2. Ensure you are in the Okta Admin application. Click on the ADMIN button on the top-right portion of the screen if it's present.
3. Under the **Applications Menu**, select **Applications**. You should see your ServiceNow application. If this is a brand new Okta instance, ServiceNow will be the only application on the list.
4. Select the *ServiceNowSSOSetup - xxxxxx* Application to view the ServiceNow App instance configuration parameters.
5. On the General tab, verify that the Login URL corresponds to your ServiceNow org URL.
6. Return to your ServiceNow instance.
    a. In ServiceNow Enterprise, go to the Multi-Provider SSO application and click on Identity Providers. Your recently-added IdP should be available in the table. Click to edit it and make sure that it's marked Active.
    b. In ServiceNow Express, you may receive an error when trying to save configuration changes to your IdP record. If so, refer to steps 7-17 in the following document: ServiceNow Support
7. Ensure that the Multi-provider SSO plugin is enabled.
    a. In ServiceNow Express, the On/Off toggle will be on the right-hand context menu when in the Authentication -> Single Sign-on application.
    b. In ServiceNow Enterprise, the On/Off setting is under the Properties section of the Multi-Provider SSO application.

3 Install and configure the Okta Active Directory agent on a domain-joined server

The Okta Active Directory (AD) agent enables Okta to import users from your internal Active Directory user store.

To install and configure the Okta AD Agent, follow these steps:

1. Read through the following section: *AD Agent Considerations* before starting the actual agent install. This section covers important concepts to understand before you begin managing users for ServiceNow.
2. Read the detailed install and configuration instructions for the AD agent in the following Okta online help page: Installing and Configuring the Active Directory Agent.

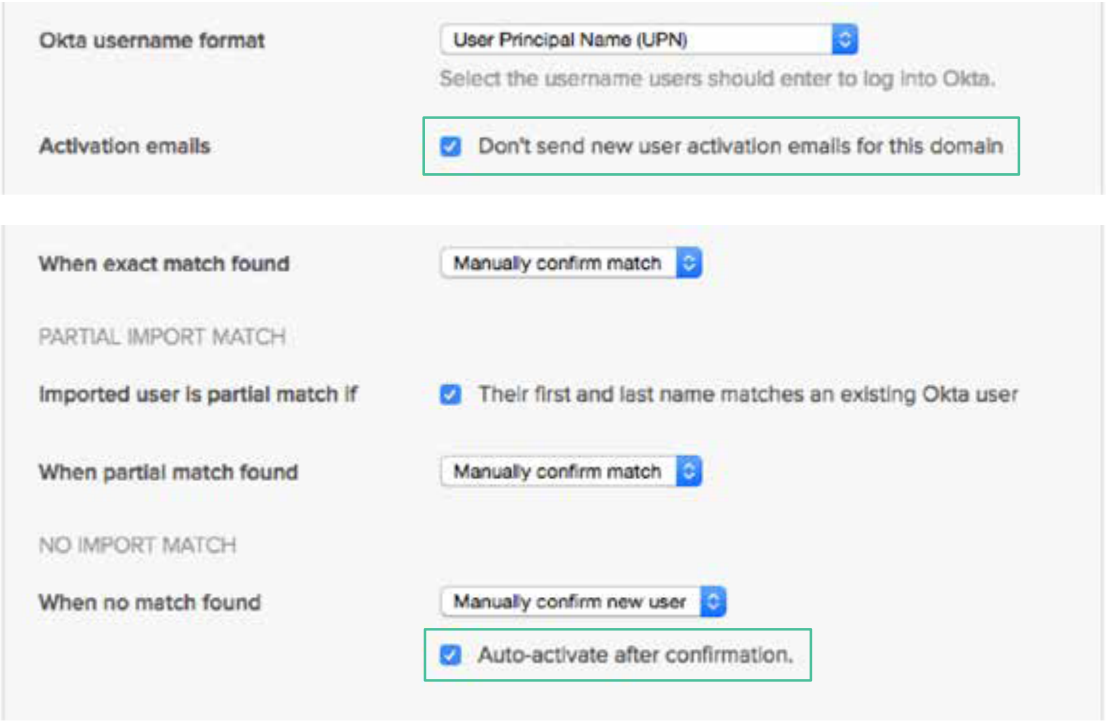
3.1 AD agent considerations

3.1.1 Activation email and auto-activate

By default, Okta is set up to send activation emails to all new Okta users. If you are mastering users from Active Directory, those emails are not needed. **Please ensure that the checkbox next to "Don't send new user activation emails from this domain" is checked.**

Similarly, as these users are coming in from Active Directory, the individual users should not have to accept or activate anything to start using Okta. **Please ensure that the "Auto-Activate after confirmation" radio button is checked.** (See Figure 5 below, which identifies both settings.)

FIGURE 5: Auto Activation and Don't Send Emails



Okta username format: User Principal Name (UPN)
Select the username users should enter to log into Okta.

Activation emails: ☑ Don't send new user activation emails for this domain

When exact match found: Manually confirm match

PARTIAL IMPORT MATCH

Imported user is partial match if: ☑ Their first and last name matches an existing Okta user

When partial match found: Manually confirm match

NO IMPORT MATCH

When no match found: Manually confirm new user
☑ Auto-activate after confirmation.

3.1.2 Import and confirmation of users

The majority of the time, you will be creating net-new Okta users from the users in Active Directory.

Once you are comfortable with the flow of new-user activations, you can automate this confirmation process by setting the Matching Rules for No Existing Match on the Settings tab. If "Auto-confirm" is selected in the drop- down box, new users from AD with no corresponding Okta record will automatically be created and available for assignment to the ServiceNow App.

Note: Leave the matching setting at "Manually Confirm" for now. (Section 6 will set up automation for this setting.)

3.1.3 Okta username format

Pay special attention to the Okta Username Format setting choice during the install of the Active Directory agent (also available from the Settings tab of your AD server once the agent is up and running). You should match this setting with what your internal users commonly use to log in to their network resources. Modern domain setups often leverage UPN (username@domain) as the username format, while older setups may still use SAMAccountName (domain\username) for legacy reasons. Documentation from Microsoft can help guide you on the differences.

Note: Okta's best practice is to match the format that your users are most familiar with.

Regardless of which format for username you chose, Okta usernames will always resemble email addresses (username@domain). However, only the username portion is required for login—as long as there are no duplicates of this username.

4 Import and Confirm Users and Groups from Active Directory

The last step during the installation of the AD agent is to run a full import from AD into Okta. You should confirm one user manually at this point to become familiar with the process. You can also test delegated authentication to AD from Okta once you have confirmed a user from AD.

1. In the Okta Administration Application, select **Directory** > **Directory Integration**.
   a. Select your AD integration in the list.
   b. Go to the **Import** tab, select **Import Now** and do a **Full Import** the first time.
   c. In the list, find a single test user from AD, select the checkbox to the far right of that user row, then click **Confirm Assignments**.
   d. In the *Confirm Imported User Assignments* dialog box, select *Auto-activate new users after user confirmation*, then click *Confirm*.
   e. Select **Directory** > **People** and verify that the user now exists in Okta.
2. Select **Directory** > **Groups** and verify that security groups from Active Directory are available in Okta.
3. From a separate browser or browser session, log in to your Okta org as the test user identified above. If you log in successfully, your username settings, AD settings, and delegated authentication are set up correctly.

5 Enable Provisioning Features in Okta for ServiceNow

Enabling user provisioning allows users to be created automatically in ServiceNow by Okta. If Okta is integrated with your Active Directory or LDAP, you can auto-provision users based on new users showing up in your directory, and control provisioning through security groups.

For most ServiceNow Okta Identity Cloud for ServiceNow application customers, allowing Okta to control both provisioning (user create) and SSO (user authentication) for ServiceNow is the desired behavior.

To enable provisioning for ServiceNow:

1. Log into Okta as an administrator.
2. Navigate to **Applications**, then select **Applications** and click on the **ServiceNow** app.
3. Select the **Provisioning** tab, then click on the **Enable Provisioning Feature** checkbox.
4. Provide the ServiceNow Admin username (typically, "Admin") and password. You can also use a separate ServiceNow user with the admin role, but it is common to use the Admin account.
5. Click **Test API Credentials.** If the username and password are valid, you will see a green success message at the top of the page. If you see an error, please validate credentials and try again.
6. Lower on the page, enable the following features:
   a. Create Users
   b. Update User Attributes
   c. Deactivate Users
7. If you want to synchronize a password with each ServiceNow user record, enable **Sync Password**. It is useful to sync passwords so that if a user accidentally tries to log into the ServiceNow "front door" using Username and Password entries, they do not lock themselves out (as they would if there were no password synced).
8. Click **SAVE** at the bottom of the screen, and verify the green "Provisioning Settings saved!" status message at the top of the screen.

5.1 Test and validate provisioning and SSO

At this point, everything should have a proper baseline setup to allow for provisioning and SSO of users into ServiceNow via Okta. To test, do the following:

1. If not logged in already, log into Okta as administrator.
2. Navigate to **Applications**, and click on the ServiceNow app.
3. Click on the **Assignments** tab, and then click the green **Assign** button.
4. Click on **Assign to People**, then click on **Assign** next to the user you imported and confirmed in Section 4.
5. Click Save and Go Back.
6. Click **Done** and verify that the user now shows up in the **Assignments** section of the ServiceNow app.
7. Open a separate tab and log into your ServiceNow instance as an admin.

8. Open the **sys_user table ('Users' in the left navbar search)** and verify that the user has been created in ServiceNow.

9. From a separate browser session (or Incognito/Private mode), log in to your Okta org as the test user.

10. Once that user gets logged into Okta, click on the **ServiceNow Chiclet** on his or her My Applications page, then verify that the user got logged into ServiceNow successfully.

    If SSO fails, see **SSO Troubleshooting** in the **Appendix** for suggestions.

5.2 Decide on which attributes to provision

The ServiceNow integration in Okta can provision any attribute in Okta into any field in the sys_user table in ServiceNow. The integration is pre-configured with a common set of default attributes that will be pushed when a user is created or updated. They are:

- first_name
- last_name
- middle_name
- email
- introduction
- title
- mobile_phone
- phone
- street
- city
- state
- zip
- county
- time_zone
- employee_number
- cost_center
- company
- department
- manager

Okta can provision user attributes into other fields in the sys_user table, as well. This includes support for custom fields that you may have added to sys_user yourself. First, you will need to Discover those attributes and add them to the ServceNow User Profile in Okta, and then you will need to map an attribute from the Okta User Profile into that attribute so that it is populated when a provisioning event occurs. As an example, let's add the sys_user field *Building* to the list of attributes that Okta will provision.

5.2.1 ServiceNow Profile Changes and Mappings

To expand the ServiceNow profile with additional attributes from sys_user:

1. As an Admin in Okta, hover over Directory and then click Profile Editor.
2. Click on the Profile button in the ServiceNow row.
3. Click on the Add Attribute button to open the Schema Discovery window. Okta will populate a list of available fields in the sys_user table.
4. Select *Home Phone*, and click Save
5. Refresh the screen on the Profile page to see the *Home Phone* attribute down at the bottom of the list of attributes in the ServiceNow User Profile in Okta.

The final step is to map an attribute from the Okta User Profile into the just-added attribute in the ServiceNow User Profile, so that when a user is provisioned into ServiceNow, the appropriate value is created in that field in sys_user. To map a user attribute from the larger Okta profile into the specific ServiceNow User Profile:

1. As an Admin in Okta, hover over Directory and then click Profile Editor.
2. Click on the Mappings button in the ServiceNow row.
    a. In this screen you establish the relationships between Okta User Profile attributes and specific-app user profiles
3. Click on "Okta to ServiceNow" in the top selector bar, to make sure we define behaviors for provisioning and not import events.
4. Scroll down and find the *Home Phone* attribute in the right-hand list.
5. In the drop-down to the left of the *Home Phone* attribute, select the Attribute that holds your building locations. For demonstration purposes, choose *firstName*.
6. Click Save. You'll be prompted to make changes to existing users – choose "Apply Updates Now"

When a user is provisioned to ServiceNow after these changes, the system will take the attribute value contained in the *firstName* attribute, and put it into the *Home Phone* field in sys_user. This method can be used to provision any attribute in Okta into any field in sys_user, including Custom fields. Don't forget to undo the mapping between firstName and Home Phone.

5.3 Provisioning considerations

It is the act of assigning a User or Group of users to the ServiceNow application in Okta that triggers provisioning into ServiceNow. If you have users assigned to the app before you enable provisioning, they will not be retro- actively provisioned. You should remove and re-add those users. Otherwise, you can now begin to assign users and groups to your ServiceNow app.

6 Determine User and Group Assignment Plan

Administrators will want to take full advantage of groups within Okta to fully automate provisioning and SSO for ServiceNow. Groups can be assigned to the ServiceNow app in Okta in exactly the same way as users were assigned. (For an example, see Section 5.1).

To set up Okta to automatically provision users to ServiceNow based on group membership, you will need to:

1. Determine a group (or set of groups) in Active Directory that will contain users that need to be created in ServiceNow.
2. Assign that group (or set of groups) to the ServiceNow app in Okta.
3. Ensure that new users from Active Directory are automatically imported and confirmed in Okta.

6.1 Determine Groups to define ServiceNow access

Successfully installing the Active Directory agent (see Section 3) will also import all security groups that are in scope into Okta. When users are confirmed from Active Directory into Okta, their group membership attributes are honored, so in Okta they will become members of any security group that they are members of in Active Directory (within scope). No additional configuration is necessary for this to work.

Administrators can leverage any group object from Okta to assign to the ServiceNow application.

Administrators are not limited to the following two scenarios, but these are two common architectures for group management with ServiceNow:

1. Build a new security group in Active Directory that defines all users who need to be provisioned to ServiceNow. By assigning this single group in Okta to the ServiceNow app, administration remains straightforward; membership in that group causes provisioning (and SSO) to ServiceNow.
2. Define groups in Active Directory to match the roles in use in ServiceNow Express. For example, having groups for “IT ADMINS” and “FRONTLINE USERS” allows for a user-based separation of roles in ServiceNow.

Once a group strategy is defined, create the groups in Active Directory and ensure they are available in Okta.
You can run a manual import from your Active Directory server page in Okta to immediately make newly created groups available in Okta.

6.2 Assign groups to ServiceNow application in Okta

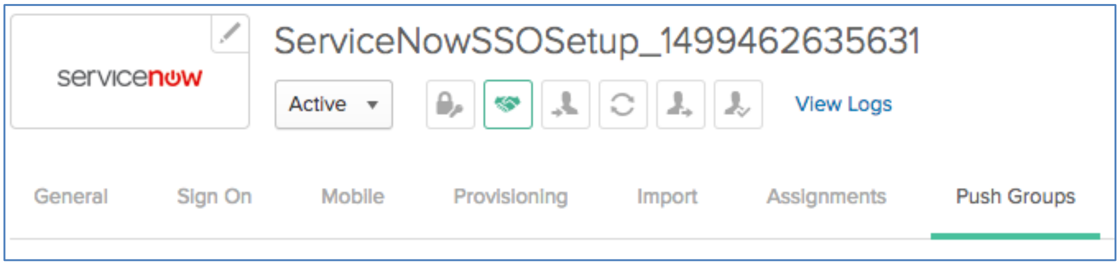
1. I If not logged in already, log into Okta as administrator.
2. Navigate to **Applications**, and click on the ServiceNow app.
3. Click on the **Assignments** tab, and then click the green **Assign** button.
4. Click Assign to Groups for the AD group that you want to assign to the application, then click Assign.

   In the pop up, set the drop-downs for Time Zone, Cost center, Company and Department to ‘not selected.’ User attribute values will be pushed for these attributes, and they do not need to be overridden at a group level.
5. Once all groups have been assigned, click Done.

6.3 Determine Push Groups strategy

Okta can also push group objects to ServiceNow. If you want to replicate group names and membership from Okta to ServiceNow, simply add the desired group to the Push Group tab in the ServiceNow application in Okta. (See Figure 6 for the location of this setting.)

Figure 6: Push Groups configuration



This configuration allows you to map an organizational structure from AD to ServiceNow, which can be helpful for highly segmented infrastructures or organizations that have large numbers of both fulfillers and submitters. Okta Push Groups will honor group membership of users whom Okta provisions. Please ensure that you map the same groups for Section 6.2 and 6.3 to control this behavior.

- Group Push will push the group objects to ServiceNow.
- Assigned Groups will push user objects and will join them to the appropriate groups from the Group Push operation.

Note: Okta cannot map the new group to a role; this must be done administratively inside of ServiceNow.

From the ServiceNow application in Okta, navigate to the Groups tab. Click on the Assign button and select the groups from Section 6.1 and Section 6.2 that you wish to use to control application access.

6.4 Automate new-user creation from Active Directory to Okta

6.4.1 Ignoring user accounts (optional)

Before automating the creation of new Okta users based on changes to Active Directory, administrators will want to clean up their user stores. There is no negative impact to having a large number of users in your Okta user store, but it is usually helpful to avoid importing service accounts, printer/computer objects, and other non- essential user accounts. You can accomplish this by ignoring those accounts from the Import tab.

1. In Okta Administrator Application, point to Directory and select Directory Integration.
2. Select the Active Directory server that you installed earlier, then click on the **Import** tab.
3. From the **Import** tab, search for an account that you wish to Ignore (ex. PRINTER1).
4. In the **Okta User Assignment** column (on the right-hand side), click the drop-down arrow and change the Confirmation Action to **Ignore**.
5. Click Confirm Assignments.

6. Click on the **Ignore** sub-tab, and verify that PRINTER1 is now on the Ignore list. This action ensures that PRINTER1 will not be added as a full Okta user.

7. Repeat the process for all users you want to not bring into Okta.

6.4.2 Automating user import and confirmation

To automate the matching of new Active Directory users to Okta users:

1. Click on the **Settings** tab, then change the setting for **No Existing Match** from Manually Confirm to
   Auto Confirm.

2. Click on the Auto Activate after Confirmation checkbox.

3. Click **SAVE**.

4. Navigate to the **Import** tab and click on the Import Now button. Run a **Full Import**.

5. All users should be automatically matched to new Okta users and should all be activated users. Point to

   Directory, then select **People** and verify.

At this point, your Okta org is set up to automatically import and confirm new users from Active Directory into Okta. If a new user is a member of a group that's been assigned to the ServiceNow application, then that user will automatically be provisioned to and enabled for SSO into ServiceNow. If the user is removed from the group in Active Directory, Okta will see that as an attribute change and will remove the user from the group in Okta, which will result in the user being deactivated in ServiceNow, fully automating the user lifecycle.

7 Install Desktop SSO (optional)

Desktop SSO can also be thought of as "credential pass-thru," allowing Okta to automatically log in a user who has already been authenticated to a domain-joined computer. This process is accomplished by leveraging the IWA service, which runs on an Internet Information Services (IIS) server and is configured specifically to work with Okta. With Desktop SSO fully configured, users trying to log in to ServiceNow via Okta will automatically be logged directly into ServiceNow and will not be prompted for credentials during the Okta authentication step.

Desktop SSO does not have any specific setup requirements with ServiceNow. Install instructions can be found on the Okta Support Center at:
https://support.okta.com/help/articles/Knowledge_Article/28101616-%20Configuring-Desktop-SSO

8 Set up High Availability (HA) for AD and Desktop SSO (IWA) Agents

Both the Active Directory and Desktop SSO agents are critical components of the infrastructure supporting Okta for provisioning and SSO. In that light, both of these agents should have a high-availability strategy applied to them.

8.1 General High Availability recommendations

Okta's best practice is to have High Availability (HA) for AD and Desktop SSO match your organization's existing policies for server HA and DR. For new setups or where such a policy is undefined, Okta recommends at least the following:

- Two servers (or virtual machines) matching the minimum configuration standards for AD and Desktop SSO agents (see install guides for minimums).
- Install *both* the AD Agent and Desktop SSO onto *both servers*. (The AD Agent will not conflict with the IWA services running under IIS.)
- Set server A as the primary server for AD and server B as the primary server for AD
- Set server B as the primary server for Desktop SSO and server A as the failover server for Desktop SSO.

This architecture will distribute normal load between Desktop SSO and AD calls across both servers, but will provide backup services in the case of server (or VM) failure.

Note: This architecture represents the minimum reasonable HA strategy for Active Directory agent and Desktop SSO services. Multiple domain infrastructures, geographically distributed user bases, and other infrastructure considerations can change HA requirements. Companies should match Okta HA decisions to their internal IT availability best practices.

8.2 High Availability for the Active Directory agent

Setting up HA for the AD service is simple. Okta will handle all agent communications failover from the cloud; if one agent is unavailable, the next agent in the list will be contacted. Therefore, setting up HA is as easy as installing another AD agent on a separate server. HA configuration is covered in the install instructions on the

Okta Support Center at: https://support.okta.com/help/articles/Knowledge_Article/28774118-Installing-and- Configuring-the-Active-Directory-Agent#ConfigHA.

8.3 High Availability for the Desktop SSO Agent

If your organization is not using Desktop SSO, please skip this section. Setting up HA for Desktop SSO is simple. Okta can programmatically check an IWA server for availability, and can be configured to check a secondary server in case of unavailability. Setup instructions for HA with Desktop SSO can be found on the Okta Support Center at: https://support.okta.com/help/articles/Knowledge_Article/28102496-Configuring-Automatic-%20Failover-for-Desktop-SSO

9 Configure Active Directory Password Reset (optional)

You can configure Okta to allow users to reset their Active Directory passwords via an Okta flow. This reset flow is commonly instantiated from the Okta org homepage or Okta user homepage, but organizations can also take the Okta password reset link from the Okta org homepage and embed it into a local portal for easy access. If Okta is configured to sync passwords with ServiceNow, this updated password can also be pushed down into the app.

Password reset does not have any specific setup requirements with ServiceNow. You'll find setup instructions on the Okta Support Center at: https://support.okta.com/help/articles/Knowledge_Article/51285468-Active-%20Directory-Password-Reset.

Appendix A—Things to Know

There are several items that cannot be prescriptively documented, as they must be decided specific to a customer implementation or with specific customer details. This section will cover these items and give guidance on how to best make those decisions for your specific implementation. It is Okta's recommendation to read this section through before you start provisioning users into ServiceNow.

Data validation in ServiceNow

Administrators often wish to populate manager, location, and department attributes from Active Directory into ServiceNow. It is important to know that these fields are validated by ServiceNow when a user is created, and therefore the values in those fields must already exist in ServiceNow before the user record is created; otherwise the fields will not populate. For example, if Frank is Bill's manager, Frank's user record needs to already exist in ServiceNow before Bill is provisioned from Okta; otherwise Bill's manager field will be blank. This same logic applies to the department and location attributes as well.

Department and location are easily managed. Administrators should ensure that all departments and locations are properly available in ServiceNow before provisioning users to the system. (You can also see Section 9.1.1 for a way to update these fields after users have been provisioned.)

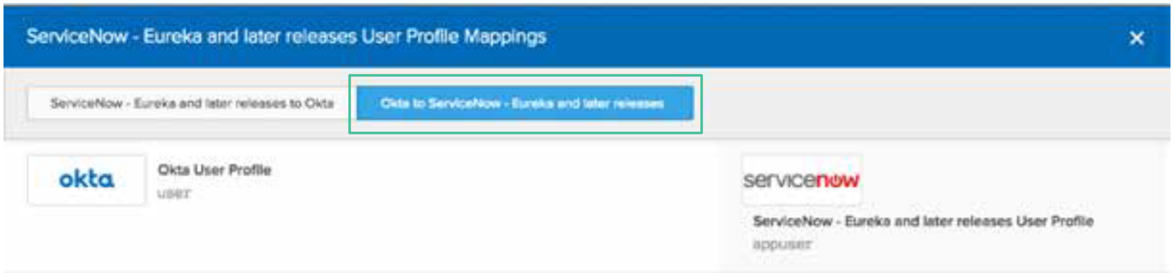
For the manager field, it is best to provision users into ServiceNow in a hierarchal way, such that managers are provisioned before their staff. However, it is not always easy to accomplish this end. For a workaround, see the next section.

Force update of attributes for already-provisioned users

Okta provides a method to update attribute values for already provisioned users. This method is useful if users have been provisioned before department, location, or manager information was properly available, which leaves those fields blank in user records. To force an update of all user record fields for all provisioned users from Okta, do the following:

1. In Okta Administrator Application, point to Applications, then select Applications and click on the **ServiceNow** app.
2. Select the **Provisioning** tab and scroll to the bottom of the page to the **Profile Attributes & Mappings**.
3. Click on Edit Mappings.
4. When the attribute mapping window loads, choose **Okta to ServiceNowSSOSetup_xxx** across the top. (See Figure 7 below for an example of this screen.)

Figure 7: Okta to ServiceNow Mapping selector (need to update screenshot)

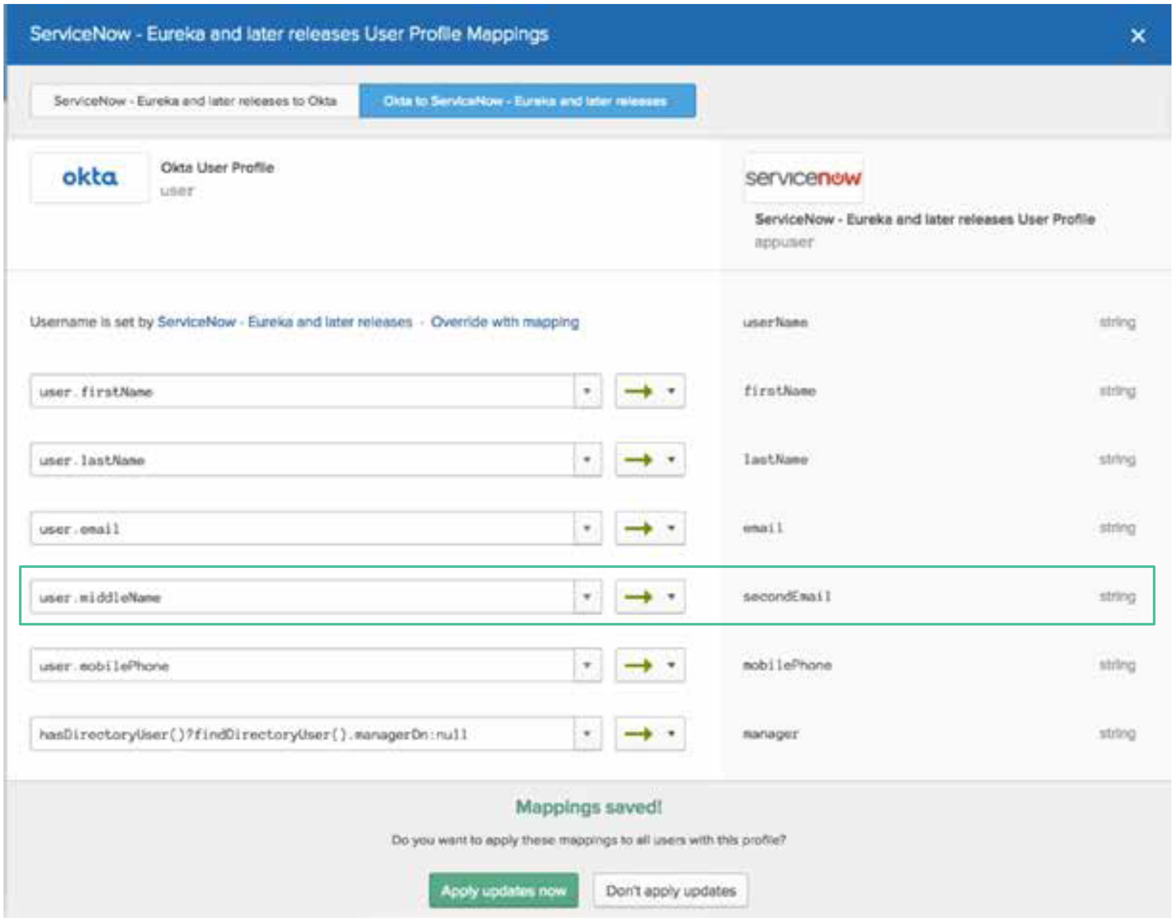

ServiceNow - Eureka and later releases User Profile Mappings
×
ServiceNow - Eureka and later releases to Okta
Okta to ServiceNow - Eureka and later releases
okta
Okta User Profile
user
servicenow
ServiceNow - Eureka and later releases User Profile
appuser

This procedure will load the ServiceNow User Profile Mappings, where administrators can map values from the Okta user profile, which is mastered by Active Directory, to the values that can be provisioned to ServiceNow. If one of these values is changed, and the new mapping is saved, Okta will update all attribute values for all users, which will result in the proper location, department, and manager values getting pushed—assuming those values now properly exist in ServiceNow.

Locate an attribute on this screen that your user records are not using. For example, if second email isn't being used in ServiceNow:

1. In the **Second Email** attribute field, click the drop-down arrow and change the attribute that's being used (for example, select **MiddleName**).
   a. See Figure 8 below.
2. At the bottom of the screen, click **Save Mappings**.
3. A popup will appear that says, "Do you want to apply these mappings to all users with this profile?"
   a. Click **YES**.
4. When the **Successful Update** message appears in Okta, all user records have been updated.
5. Change the attribute from #1 back to its original value to preserve future functionality, and save the mapping again.

Figure 8: Changed users second email attribute to force profile update


ServiceNow - Eureka and later releases User Profile Mappings
ServiceNow - Eureka and later releases to Okta
Okta to ServiceNow - Eureka and later releases
okta
Okta User Profile
user
servicenow
ServiceNow - Eureka and later releases User Profile
appuser

Username is set by ServiceNow - Eureka and later releases · Override with mapping

	userName	string
user.firstName	firstName	string
user.lastName	lastName	string
user.email	email	string
user.middleName	secondEmail	string
user.mobilePhone	mobilePhone	string
hasDirectoryUser()?findDirectoryUser().managerDn:null	manager	string

Mappings saved!

Do you want to apply these mappings to all users with this profile?

In ServiceNow, validate that a user's manager, department, or location is now properly updated.

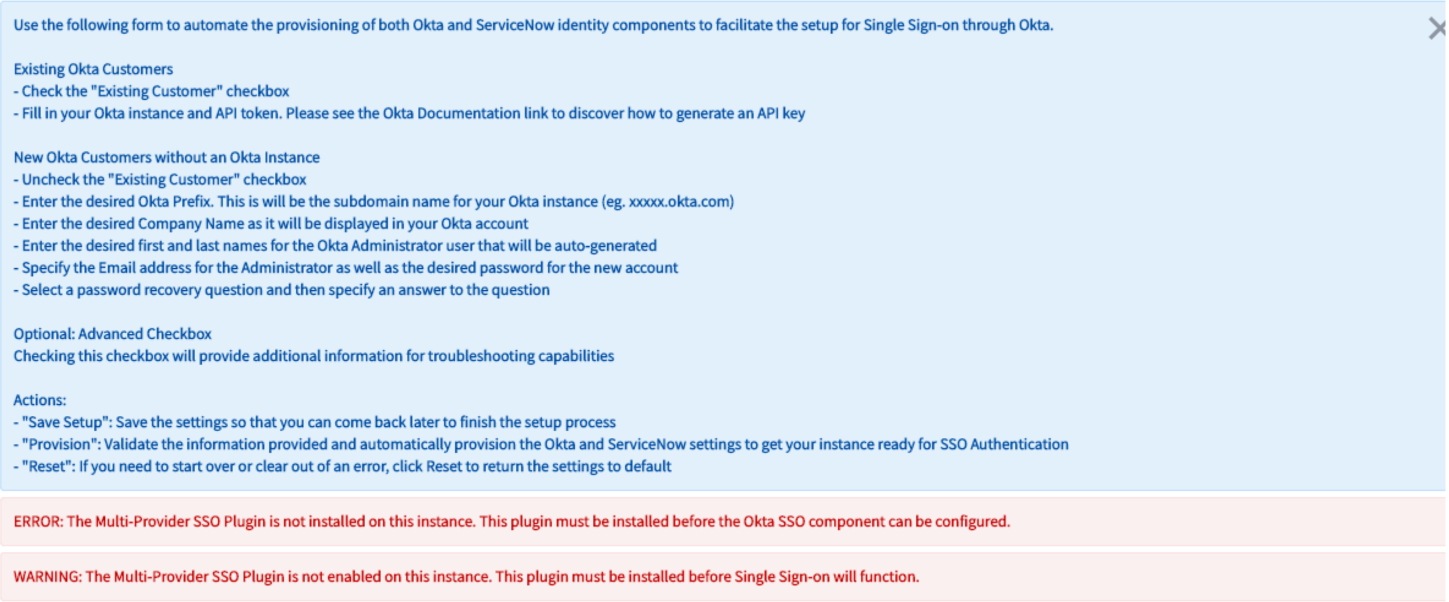
User appears in Okta, but is not provisioned to ServiceNow

When a user is assigned to the ServiceNow app instance in Okta, if provisioning is enabled, that user is then immediately provisioned down to the app. If users are not provisioned down to ServiceNow from Okta, check the following:

1. In the **Okta Administrator Application**, check the **Dashboard** first for push profile error messages.
2. Ensure that provisioning is enabled in the ServiceNow app instance. See Section 5 for setup guidance.
3. Ensure that any users assigned to the ServiceNow app instance have been assigned after provisioning was enabled for the app.
   a. It is nondestructive to remove and re-add users to the ServiceNow app instance in Okta.
   b. Remove and reassign the user in question from the People sub-tab –OR—
   c. Remove and reassign the user group in question from the Groups sub-tab.
4. If the user does not provision after trying #1 and #2 above, please contact your ServiceNow or Okta rep for assistance.

Multi-provider plugin is required

If the multi-provider SSO plugin is not enabled in your ServiceNow instance, the Okta SSO plugin will surface an error message. This message will go away once the Multi-Provider SSO plugin is installed and activated in ServiceNow.



Use the following form to automate the provisioning of both Okta and ServiceNow identity components to facilitate the setup for Single Sign-on through Okta.

Existing Okta Customers
- Check the "Existing Customer" checkbox
- Fill in your Okta instance and API token. Please see the Okta Documentation link to discover how to generate an API key

New Okta Customers without an Okta Instance
- Uncheck the "Existing Customer" checkbox
- Enter the desired Okta Prefix. This is will be the subdomain name for your Okta instance (eg. xxxxx.okta.com)
- Enter the desired Company Name as it will be displayed in your Okta account
- Enter the desired first and last names for the Okta Administrator user that will be auto-generated
- Specify the Email address for the Administrator as well as the desired password for the new account
- Select a password recovery question and then specify an answer to the question

Optional: Advanced Checkbox
Checking this checkbox will provide additional information for troubleshooting capabilities

Actions:
- "Save Setup": Save the settings so that you can come back later to finish the setup process
- "Provision": Validate the information provided and automatically provision the Okta and ServiceNow settings to get your instance ready for SSO Authentication
- "Reset": If you need to start over or clear out of an error, click Reset to return the settings to default

ERROR: The Multi-Provider SSO Plugin is not installed on this instance. This plugin must be installed before the Okta SSO component can be configured.

WARNING: The Multi-Provider SSO Plugin is not enabled on this instance. This plugin must be installed before Single Sign-on will function.

SSO fails and returns user to ServiceNow login screen

By default, the IdP record created by the OIC app will look at the ‘email’ field in ServiceNow to match username. If you’re provisioning username as something other than email (or email-like), you’ll want to change this to match your format.

If there's a username mismatch, the SAML connection opens a tab with ServiceNow appropriately, but doesn't log in and cycles back to the normal ServiceNow login page. You may also see a red error message briefly from ServiceNow that says 'User: john.doe@domain.com" doesn't exist', even though that's the user you're trying to log in. If you've verified that the user DOES exist in the sys_user table, check this setting.

Service-provider initiated (SP-init) Logins

For SP-initiated logins into ServiceNow, configuration is different between Express and Enterprise.

For ServiceNow Express, if you set the "Primary" toggle on the identity provider record, any user that browses to the ServiceNow home page will automatically be redirected to an Okta login page.

For ServiceNow Enterprise, please follow the directions available from the SAML Setup Instructions link, available from the sign-on tab of your ServiceNow application. Those instructions can be directly found here as well - http://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-ServiceNow.html?baseAdminUrl=https://exp1-admin.okta.com&app=servicenow_ud&instanceId=0oa314btz3gQKOGAz1t7.

Configuring Single-Log Out (SLO)

SLO only applies to ServiceNow Enterprise. To configure your Okta tenant for SLO, please follow the directions available from the SAML Setup Instructions link, available from the sign-on tab of your ServiceNow application. Those instructions can be directly found here as well - http://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-ServiceNow.html?baseAdminUrl=https://exp1-admin.okta.com&app=servicenow_ud&instanceId=0oa314btz3gQKOGAz1t7.

For information concerning the general Multi-Provider SSO plug-in for ServiceNow Enterprise and its configuration with Okta as an identity provider (IdP), please refer to the SAML Setup Instructions available from within your Okta org when setting up the ServiceNow Universal Directory ('ServiceNow UD') integration, or see instructions available on the Okta Support pages (link here).

**Note – As of June 28th, Okta has released a new ServiceNow integration which fully supports Okta's Universal Directory functionality. The older 'ServiceNow – Eureka and Later' application will be deprecated at some point in the future, and although it remains functional any new configurations should leverage the new 'ServiceNow UD' application in Okta. The OIC App will provision the new integration in Okta, so anyone using the app from the ServiceNow store will receive the proper configuration.