One Identity Starling Two-Factor RADIUS Agent 7.3

Administration Guide

Starling Two-Factor RADIUS Agent Administration Guide
Updated - June 2020
Version - 7.3

Contents

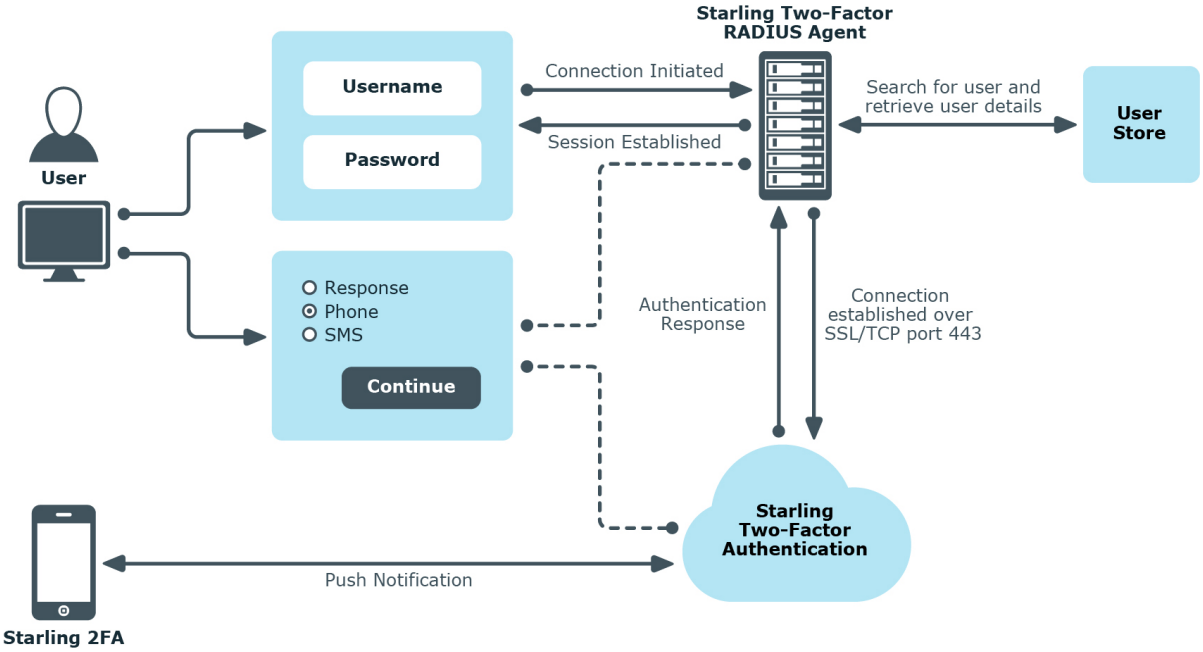
1

Overview

The One Identity Starling Two-Factor RADIUS Agent utilizes the RADIUS protocol for Two-Factor authentication (push notification or one-time password authentication) through Software as a Service (SaaS). The Starling Two-Factor RADIUS Agent can be used on SaaS and on-premises applications.

Network diagram

Figure 1: Starling Two-Factor RADIUS Agent Network Diagram



If you have an application that uses RADIUS, you can use the Starling Two-Factor RADIUS Agent as a Software as a Service for two-factor authentication. The Starling Two-Factor RADIUS Agent forwards the authentication requests from the customer application to Starling Two-Factor Authentication. Starling Two-Factor Authentication validates the requests and responds to the applications with an appropriate authentication response (Access-Accept, Access-Reject, or Access-Challenge).

Installing Starling Two-Factor RADIUS Agent

The following sections brief about the prerequisites and the steps to download and install the latest version of the **Starling Two-Factor RADIUS Agent**.

Prerequisites for installation

The following are the prerequisites for installing the Starling Two-Factor RADIUS Agent:

- Microsoft .NET Framework 4.6.1 or later
- Starling Two-Factor Authentication subscription
- A valid mobile number and email address configured for the user

Downloading and running the Starling Two-Factor RADIUS Agent

The following sections briefs about the steps to download and install the latest version of the **Starling Two-Factor RADIUS Agent**.

To download the installer

1. On the support.oneidentity.com site, sign in to the One Identity account by entering credentials. If you do not have an account, click **Sign up for a new account**. You also have the option of signing in through the Microsoft account.

   The **One Identity Support page** is displayed.

2. In the **Identity as a Service** section, click **Starling Two-Factor Authentication**.

   The **Product Support - Starling Two-Factor Authentication** page is displayed.

3. Click **Install & Upgrade** tab.
4. Click **Starling Two-Factor RADIUS Agent 7.3**.

   The **Download Starling Two-Factor RADIUS Agent 7.3** page is displayed.

5. Click **Add to Downloads**.
6. Review the terms and conditions and click **Continue**.

   The **Add to My Downloads** page is displayed.

7. Click **Download Now** to download the `.zip` file.
8. Click **Add to My Downloads** to save the application in the **My Downloads** cart. It is recommended to use this option when you are downloading multiple products.

   The StarlingTwoFactorRADIUSAgent.zip file is downloaded.

To run the installer

1. Extract the downloaded StarlingTwoFactorRADIUSAgent.zip file to your local drive.

   The extracted folder contains **Setup.exe** and **StarlingTwoFactorRADIUSAgent.msi** files.

2. Right click **Setup.exe** file and click **Run as Administrator**.
3. Follow the instructions on the installer screens to complete the installation.

NOTE: Once the installation is complete, configure Starling Two-Factor RADIUS Agent settings. For details, see the Starling Two-Factor RADIUS Agent configuration.

The account under which you will be running the Setup must be a member of the local administrators group.

IMPORTANT: In case of an upgrade from Starling Two-Factor RADIUS Agent 6.x to 7.3, you must connect to Starling as the Subscription key related provision is removed. Connect to Starling using the credentials that were used to create the Starling account. All configurations that were part of the earlier version of RADIUS Agent will be retained after the upgrade. For information on connecting to Starling, see Connecting Starling for authentication.

3

Starling Two-Factor RADIUS Agent configuration

You can configure the Starling Two-Factor RADIUS Agent for two-factor authentication by setting the required parameters in the **Starling Two-Factor RADIUS Agent Configuration** window. You can set the parameters using the following options that are displayed on the **Starling Two-Factor RADIUS Agent configuration** window:

- **Home**: Displays the various configuration options in a tree view and as tiles.
- **Server Settings**: Allows you to configure the RADIUS server by providing the IP address and port number.
- **Connect Starling**: Allows you to connect to the Two-Factor Authentication subscription by logging in to your One Identity Starling account.
- **Push Notification**: Allows you to configure the push notifications messages and timeout settings.
- **User Repository**: Allows you to specify the repository for storing the user data. The available options are **Active Directory** or as a **comma-separated values** (CSV).
- **Client Settings**: Allows you to configure the RADIUS clients who need to be authenticated using the Starling Two-Factor authentication.

Configuring RADIUS Agent server

To configure the RADIUS Agent server settings

1. In the **Server Settings** section on the Starling Two-Factor RADIUS Agent Configuration window, provide the following details:
    - **IP address**: IP address of the RADIUS Agent server, that validates the authentication requests. The field lists all the IP addresses (IPv4 addresses) on the server and displays the first server in the list. Select the IP that you want to use for authentication.
    - **Port number**: The port number that the RADIUS Agent will use to receive the authentication requests. The default port is 1812. You must configure the

firewall exceptions manually to allow Starling Two-Factor RADIUS Agent traffic on the selected port.

2. After completing the configuration, click **Save Settings**.

   The **Starling Two-Factor RADIUS Agent configuration** dialog is displayed prompting you to restart the service.

3. Restart the Starling Two-Factor RADIUS Agent service to save the changes.

Connecting Starling for authentication

To use the Starling Two-Factor authentication for RADIUS Agent, you must first connect to Starling using the **Starling Join** option available for One Identity on-premises products.

To obtain a Starling Two-Factor Authentication subscription and register with Starling, click https://www.cloud.oneidentity.com/.

NOTE: If you do not have a Starling account, you can create a new account. For more information on creating a Starling account, see the *One Identity Starling User Guide*.

To connect to Starling for authentication, see:

- Prerequisites to connect to Starling
- Connecting RADIUS Agent to Starling

Prerequisites to connect to Starling

The following are the prerequisites to connect to Starling:

- User must have One Identity Starling account. For more information on creating a One Identity Starling account, see the *Starling Two-Factor Authentication Administration Guide*.
- The Starling Account must be activated with a valid Two-Factor Authentication subscription.

Connecting RADIUS Agent to Starling

After the pre-requisites to connect to Starling are met, connect RADIUS Agent to Starling using the **Starling Join** option available for One Identity on-premises products.

To connect and configure One Identity Starling for authentication

1. On the Starling Two-Factor RADIUS Agent configuration window, click **Connect Starling**.

   The **Connect Starling** window is displayed.

2. Click **Connect my account**.

   You are redirected to the **One Identity Starling** authentication window.

3. Provide your Starling credentials and click **SIGN IN**.

4. In the **Join to Starling** window, click **Allow**.

   NOTE: If you are a member of more than one Starling organization, use the drop-down to select the organization to which you want to connect.

5. Click **Join**.

   After successful authentication, you are redirected to the One Identity Starling Two-Factor Authentication **Connect Starling** window.

   NOTE: To connect to a different organization in your One Identity Starling account, click **Change Account**.

   If the connection is unsuccessful, a message is displayed providing the details of the error and the previously connected account is continued to be used. In such a case, it is recommended to contact support for any help.

NOTE: If there are any network issues or if the Starling is down, your account may get disconnected. In such cases, click **Reconnect**. To test the validity of your account connection, click **Test connection**.

Configuring Push notification settings

Push notification enables you to Approve or Deny login requests. These requests facilitate an end-to-end encrypted communication between the application and a secured authentication service. Accurate configuration of the push notification allows you to **Approve** or **Deny** a login attempt.

To configure the push notification settings

1. On the **Starling Two-Factor RADIUS Agent configuration** page, click **Push Notification**.

   Push Notification window is displayed.

2. On the **Message** field, enter a message to be displayed in the Starling Two-Factor application. The message entered must be in the range of 10 to 50 characters.

3. On the **Timeout (seconds)** field, select the timeout duration or the validity of the notification from the drop-down menu. If you select **Other**, you can specify the customized timeout duration in seconds. By default, 30 seconds is set as a timeout

duration for notifications.

4. Click **Save Settings** after completing the configuration.

Configuring user repository

You can configure the user repository details in the **User repository** section depending on the option used for storing user data. The user data can be stored either in the Active Directory or in a CSV file.

Prerequisites to configure user repository

The following are the prerequisites to configure the user repository:

- A domain controller must exist.
- User must have the minimum read permission to query the Active Directory and read user data.

Configuring user repository for Active Directory

If the user data is stored in Active Directory, you must configure the Starling Two-Factor RADIUS Agent to access the user data.

To configure RADIUS Agent to access user data stored in Active Directory

1. On the **Starling Two-Factor RADIUS Agent configuration** page, click **User Repository**.

   The **User Repository** window is displayed.
2. Select the required option to store the user data. By default, the **Use Active Directory** option is selected.
3. Provide the following parameters:
   - **Domain name**: Name of the Active Directory domain.
   - **User name**: User account used for querying the Active Directory.
   - **Password**: Password of the account used for querying the Active Directory.
   - **Base DN**: This is the path from where user search is performed. You must specify the root container to search the users in the format **cn=users,dc=domain,dc=com**, where **cn** is Common Name and **dc** is Domain Component. If Base DN is not specified, the entire directory is

searched to locate the users. Active Directory users who do not belong to the specified Base DN are not authenticated using two-factor authentication.

- **Use SSL**: Option to enable LDAP over SSL for RADIUS server to communicate with Active Directory server.
- **Perform Primary Authentication**: This allows RADIUS clients to perform primary authentication via Active Directory before an authentication happens via Starling Two-Factor Authentication.
- **Advanced Settings**: This allows the RADIUS server to modify the Active Directory attribute mapping. These attribute values are used during authentication. You can update the Active Directory attribute fields in the **Active Directory Advanced Settings** window as per the requirement. In the window, you can map **Name**, **Email**, and **Phone Number** to the attributes in Active Directory. The username entered in the client application will be validated against the **Name** attribute during two-factor authentication. By default, **Name** is mapped to the **samAccountName** attribute in Active Directory.

2. Click **Save Settings** after completing the configuration.

NOTE: If the domain name, user name, or password is invalid, an error message is displayed when you click **Save Settings**.

Configuring user repository for CSV file

If the user data is stored in CSV file, you must configure the Starling Two-Factor RADIUS Agent to access the user data.

To configure RADIUS agent to access user data stored in CSV file

1. On the **Starling Two-Factor RADIUS Agent configuration** page, click **User Repository**.

   The User Repository window is displayed.

2. Select **Use CSV file** to store the user data. By default, the **Use Active Directory** option is selected.
3. In the **File Path** field, enter the absolute path to the .csv file or click **Browse** to select the .csv file.

   NOTE:

   - The CSV file must have a header row with the following parameters in the following order: UserName, PhoneNumber, and EmailAddress.
   - The rows following the header row must contain values pertaining to each parameter in the header row. The values entered must be comma separated without quotation marks.

- If the CSV file is edited during an operation, the file must be saved and the service need not be restarted to pick the entered values.

4. Click **Save Settings** after completing the configuration.

RADIUS client configuration

You can configure the RADIUS clients to be authenticated by providing the client details in the **Client Settings** window.

Adding RADIUS clients

You can add new RADIUS clients to be authenticated through Starling Two-Factor authentication.

To add client details

1. On the **Starling Two-Factor RADIUS Agent configuration** page, click **Client Settings**.

   The **Client Settings** window is displayed.

2. Click **Add** and provide the following details:
   - **IP address**: IP address or the range of IP addresses from which the Starling Two-Factor RADIUS Agent accepts authentication requests.
     For example:
     - 192.168.70.9: In this case, the Starling Two-Factor RADIUS Agent allows authentication requests only from this IP address.
     - 192.168.70.0: If a subnet mask is entered in the **Subnet Mask** field, for example, 255.255.255.0, then Starling Two-Factor RADIUS Agent allows authentication requests from any IP address on the 192.168.70.0 subnet.
   - **Subnet mask** (Optional): If you want to specify a range of IP addresses, you have to enter the subnet mask.

     NOTE: If an invalid IP address or subnet mask is configured, authentication requests do not reach the Starling Two-Factor RADIUS Agent server and you cannot access the required resources.
   - **Shared secret**: The key that the RADIUS client uses when attempting to establish a connection with the Starling Two-Factor RADIUS Agent. The client and Starling Two-Factor RADIUS Agent must have the same shared secret. The shared secret helps to maintain the security between the Starling Two-Factor RADIUS Agent server and the RADIUS client.
3. Click **Add**.
4. On the **Client Settings** window that is displayed, click **Add** to add more clients, or

click **Save Settings** to apply the client settings changes.

A message is displayed confirming that the clients settings are updated.

Removing RADIUS clients

You can remove RADIUS clients that do not need to be authenticated through Starling Two-Factor authentication.

To remove a client

1. On the **Starling Two-Factor RADIUS Agent configuration** page, click **Client Settings**.

   The **Client Settings** window with the list of clients added for authentication is displayed.

2. Select the required client IP address or subnet mask, and click **Remove**.

   A message is displayed prompting you to confirm if you want to remove the specified client.

3. Click **Yes**.

   The Client Settings window with the specified client removed is displayed.

4. Click **Save Settings** to apply the client settings changes.

   A message is displayed confirming that client settings are updated.

Updating RADIUS clients

You can update the IP address, subnet mask, or shared secret details for the RADIUS clients that are added to be authenticated through Starling Two-Factor authentication.

To update the client details

1. On the **Starling Two-Factor RADIUS Agent configuration** page, click **Client Settings**.

   The **Client Settings** window with the list of clients added for authentication is displayed.

2. Select the required client IP address or subnet mask, and click **Update**.

   The Update RADIUS Client window with the details of the selected client is displayed.

3. Update the required details, and click **Update**.

   The Client Settings window with the updated client details is displayed.

4. Click **Save Settings** to apply the updated client settings.
   A message is displayed confirming that the clients settings are updated.

Integrating Starling Two-Factor RADIUS Agent in applications

You can integrate any applications which require two-factor authentication in your organization with the Starling Two-Factor RADIUS Agent server. To integrate the application with the RADIUS Agent server you must perform the following configurations in the applications.

To configure Starling Two-Factor RADIUS Agent in the application

1. Launch the application, which requires RADIUS Agent server integration.
2. Configure the Starling Two-Factor RADIUS Agent authenticator into the application by providing the following values:
    - RADIUS server IP address
    - Port number
    - Shared secret key

For more information about integration, see the documentation for the application, which is being integrated with RADIUS Agent server.

5

Logging into the application using RADIUS authenticator

To log in to the application, which is integrated with RADIUS Agent server, you can use OTP or push notifications for two-factor authentication.

When you log in to the application for the first time, during two-factor authentication, you will receive an SMS to install the Starling 2FA app if:

- You have not installed the Starling 2FA app.
- The **Installation Instructions** option in the Starling Two-Factor Authentication Dashboard is enabled.

NOTE: On the RADIUS Agent configuration tool, if the **Perform Primary Authentication** option is selected, then enter the Active Directory (AD) user password in the **Password** field. After the password is validated against AD, perform the two-factor authentication using the OTP or the push notifications methods.

You can perform the two-factor authentication using one of the following methods:

- OTP through SMS
- OTP through phone call
- OTP through Starling 2FA app
- Push notifications in Starling 2FA app

OTP through SMS

To perform two-factor authentication when you log in to the application using OTP through SMS method, you must have a valid mobile number to receive the token response via SMS for authentication.

To generate OTP through SMS

1. On the application being integrated with RADIUS Agent server, in the token response field, enter **SMS** .

2. Click **Enter**.

   You will receive an SMS on the registered mobile number.
3. In the token response field of the application, enter the OTP received through SMS.
4. Click **Enter** to log in to the application.

OTP through phone call

To perform two-factor authentication when you log in to the application using OTP through phone call method, you must have a valid mobile phone number to receive the token response via a phone call for authentication.

To generate OTP through phone call

1. On the application being integrated with RADIUS Agent server, in the token response field, enter **Phone** .
2. Click **Enter**.

   You will receive a phone call on the registered mobile number.
3. In the token response field of the application, enter the OTP received through the phone call.
4. Click **Enter** to log in to the application.

OTP through Starling 2FA app

To perform two-factor authentication when you log in to the application using OTP through the Starling 2FA application, you must have the Starling 2FA app installed on your mobile device or on Desktop to receive the token response code for authentication.

NOTE: The Starling 2FA app can be used for two-factor authentication on Android or iOS devices for Mobile versions, and the Windows or Macintosh for Desktop versions.

To generate OTP through Starling 2FA app if you are a new user

1. On the application being integrated with RADIUS Agent server, in the token response field, do not enter any value and click **Enter**.
   - If you have installed the Starling 2FA app, then your token will be added to the app.
   - If you have not installed the Starling 2FA app, install the mobile app and register your mobile phone number. Install the app either from the SMS you have received or from the app store. After installing the Starling 2FA app, your token will be added to the app.

You will receive a phone call on the registered mobile phone number.

2. In the token response field of the application, enter the OTP received from the token in the Starling 2FA app.
3. Click **Enter** to log in to the application.

To generate OTP through Starling 2FA app if you are an existing user

1. On the application being integrated with RADIUS Agent server, in the token response field, do not enter any value and click **Enter**.
2. In the token response field of the application, enter the OTP received from the token in the Starling 2FA app.
3. Click **Enter** to log in to the application.

Push notifications in Starling 2FA app

To perform two-factor authentication when you log in to the application using push notifications in the Starling 2FA application, you must have the Starling 2FA app installed on your mobile device or on Desktop, and your mobile phone number must be registered with the app.

NOTE: The Starling 2FA app can be used for two-factor authentication on Android or iOS devices for Mobile versions, and the Windows or Macintosh for Desktop versions.

To use push notifications

1. If you have not installed the Starling 2FA app, install the app from the app store or using **Get the app** link (https://2fa.cloud.oneidentity.com/install).
2. On the application being integrated with RADIUS Agent server, in the token response field, enter **Push**.
3. Click **Enter**.

   You token will be added to the Starling 2FA app.
4. Open the Starling 2FA app and navigate to the **Requests** menu.
5. In the **Pending** tab, approve the request to log in to the application.

6

Diagnostic logging

To troubleshoot issues that may occur during authentication with the Starling Two-Factor RADIUS Agent, you must enable diagnostic logging for the Starling Two-Factor RADIUS Agent. By default, diagnostic logging is disabled. After enabling or disabling diagnostic logging, you must restart the Starling Two-Factor RADIUS Agent service.

Enabling diagnostic logging

To enable diagnostic logging for Starling Two-Factor RADIUS Agent

1. On a computer where the Starling Two-Factor RADIUS Agent is installed, go to the **Starling Two-Factor RADIUS Agent** folder in the installation directory default path (*%ProgramFiles%\One Identity\Starling Two-Factor RADIUS Agent*).
    a. On a computer where the Starling Two-Factor RADIUS Agent version lesser than 7.x installed, make the following changes to the **StarlingTwoFactor.RadiusAgent.Service.exe.config** file:
        i. In the *<log4net debug="false">* entry, set the value to *"true".* For example*, <log4net debug="true">*
        ii. In the *<level value="ERROR" />* entry, set the value to *"DEBUG"*. For example, *<level value="DEBUG" />*
    b. On a computer where the Starling Two-Factor RADIUS Agent version 7.x or later is installed , make the following changes to the **log4net.config** file:
        i. In the *<log4net debug="false">* entry, set the value to *"true".* For example, *<log4net debug="true">*.
        ii. In the *<level value="ERROR" />* entry, set the value to *"DEBUG"*. For example, *<level value="DEBUG" />*.
2. Restart the Starling Two-Factor RADIUS Agent Service.

NOTE: While upgrading from Starling Two-Factor RADIUS Agent earlier versions to version 7.x, the debug logging settings are reset.

Disabling diagnostic logging

To disable diagnostic logging for Starling Two-Factor RADIUS Agent

1. On a computer where the Starling Two-Factor RADIUS Agent is installed, go to the **Starling Two-Factor RADIUS Agent** folder in the installation directory (*%ProgramFiles%\One Identity\Starling Two-Factor RADIUS Agent*)
2. On a computer having the Starling Two-Factor RADIUS Agentversion lesser than 7.x installed, make the following changes to the **StarlingTwoFactor.RadiusAgent.Service.exe.config** file:
    a. Set the *<log4net debug>* entry value to *"false".*
    b. Set the *<level value="ERROR" />* entry to *"ERROR"*.
3. On a computer having the Starling Two-Factor RADIUS Agentversion 7.x or later installed , make the following changes to the **log4net.config** file:
    a. Set the *<log4net debug>* entry value to *"false"*..
    b. Set the *<level value="ERROR" />* entry to *"ERROR"*.
4. Restart the Starling Two-Factor RADIUS Agent Service.

Uninstalling Starling Two-Factor RADIUS Agent

The following sections briefs about the steps to uninstall the **Starling Two-Factor RADIUS Agent**.

To uninstall the Starling Two-Factor RADIUS Agent

1. Navigate to **Programs and Features** in **Control Panel**, and then click **One Identity Starling Two-Factor RADIUS Agent**.
2. Click **Uninstall**.

NOTE: Once One Identity Starling Two-Factor RADIUS Agent is uninstalled, details regarding the Starling Two-Factor RADIUS Agent gets deleted from the Starling account.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product