One Identity Starling Two-Factor RADIUS Agent 7.0

Administration Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Starling Two-Factor RADIUS Agent Administration Guide
Updated - February 2019
Version - 7.0

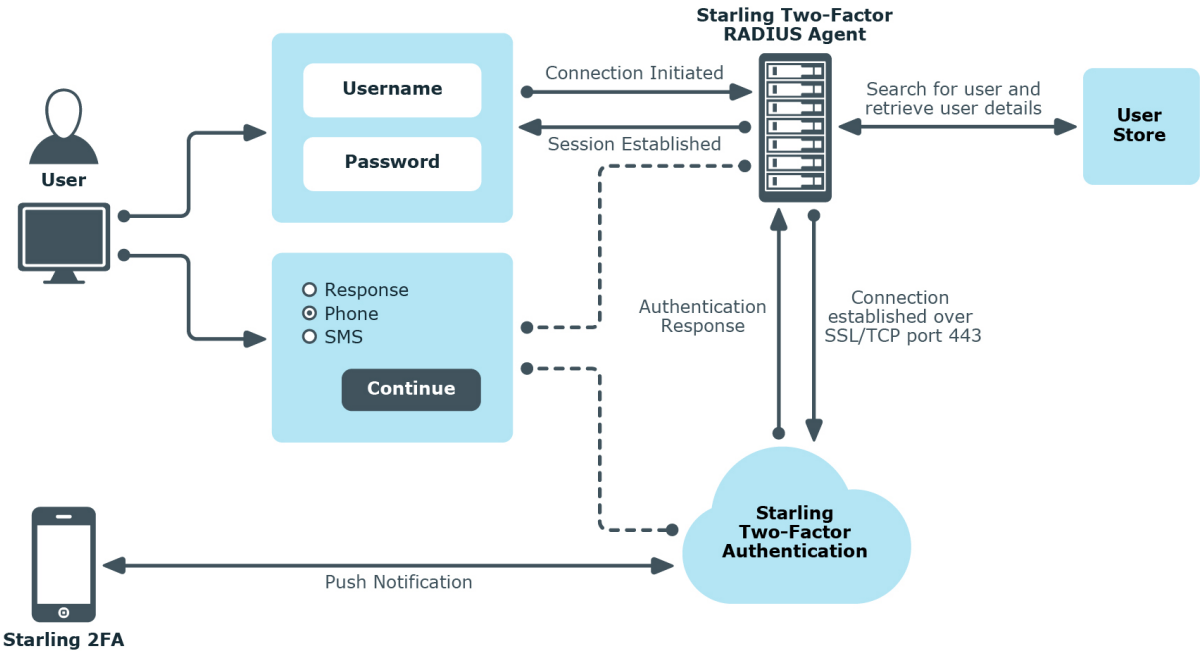
Contents

1

Overview

One Identity Starling Two-Factor RADIUS Agent provides a RADIUS-compatible solution for two-factor authentication (one-time password authentication) through Software as a Service. Starling Two-Factor RADIUS Agent can be used on SaaS and on-premise applications that use RADIUS protocol for authentication.

Network diagram



If you have an application that can be configured to use RADIUS, you can use Starling Two-Factor RADIUS Agent as a Software as a Service for two-factor authentication. 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).

Prerequisites

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

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

Running the installer

To run the installer:

- Double-click the installer and follow the instructions on the installer screens and complete the installation.

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

Starling Two-Factor RADIUS Agent configuration

You can configure Starling Two-Factor RADIUS Agent for two-factor authentication by setting the required parameters in **Starling Two-Factor RADIUS Agent Configuration** window. The configuration window allows you to configure the RADIUS Agent sever details, your Starling Two-Factor Authentication subscription details, push notification details, user repository details and the client details. These details are required to carry out two-factor authentication.

Configuring RADIUS Agent server

To configure Server settings

In the **Server Settings** section, provide the following details:

- **IP address**: IP address of RADIUS Agent server, which will be validating the authentication requests. The field lists all the IP addresses (ipv4 addresses) on the server and displays the first server in the list. You can select the IP that you want to use for authentication.
- **Port number**: The port number, which RADIUS Agent will be using to receive authentication requests. The default port is 1812. You must manually configure the firewall exceptions to allow Starling Two-Factor RADIUS Agent traffic on the selected port.

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

NOTE: The Starling Two-Factor RADIUS Agent service must be restarted to save the changes. On clicking **Save Settings**, the **Starling Two-Factor RADIUS Agent configuration** dialog appears, prompting the user to restart the service.

Connecting with Starling for Authentication

NOTE: To obtain a Starling Two-Factor Authentication subscription, click the following link: https://www.cloud.oneidentity.com/

To configure One Identity Starling for authentication

1. On the Starling Two-Factor RADIUS Agent window, click **Connect Starling**. The **Connect Starling** window is displayed.
2. Click **Connect my account**. You are redirected to **One Identity Starling** authentication window.
3. Provide your Starling credentials and click **Sign in**.

   If you are a member of more than one Starling organization, choose the organization you want to connect to, from the dropdown box. Click **Connect**.

After successful authentication, you will be redirected back to One Identity Starling Two-Factor Authentication **Connect Starling** window. You can connect to a different organization in your One Identity Starling account by clicking **Change Account**. If the process of changing accounts is not successful, the previously connected account will be used.

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

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

NOTE: If you have a Starling account when trying to join Starling, you will receive a Starling invitation email. Click the link in the email and log in to the Starling account. If your Starling account belongs to multiple organizations, you can select the organization to which Starling Two-Factor RADIUS Agent must be joined.

NOTE: If you do not have a Starling account, while you are trying to join to Starling, you will get a Starling Sign-Up email to complete a registration process to create a Starling account. Complete the registration and login using the credentials that you have provided during registration. For account creation details, see the *One Identity Starling User Guide*.

Push Notifications

Push notifications enable Starling 2FA mobile app to receive requests to approve an authentication attempt. Configuration of push notifications facilitate an end-to-end encrypted communication between the application and a secured authentication service. Accurate configuration of push notification enables the user to **Approve** or **Deny** a login attempt. Push notifications are configured by default.

Configure the following Starling Two-Factor Authentication push notification settings:

- **Message**: This is the message that would be displayed in the Starling 2FA app. The character limit for the message is mentioned below:
  - The message must comprise of less than or equal to 50 characters.
  - The message must comprise of more than or equal to 10 characters.
- **Timeout (seconds)**: Timeout determines the duration for which the push notification request received on Starling 2FA app is valid. For example, if the value of the timeout is set as 30 seconds, the validity of the notification would last for 30 seconds only. The value can be selected from the drop-down menu. If **Other** is selected from the drop-down menu, the timeout value must be entered in the **Other** field that appears below the drop-down menu. The **Other** option is provided so that a user can customize the timeout value. The default value for timeout is 30 seconds.

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

User repository configuration

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

NOTE: Currently, Starling Two-Factor RADIUS Agent supports data stored in Active Directory (LDAP) and CSV files.

Configuring user repository for Active Directory

To configure the repository for data stored in Active Directory:

1. Click the **User repository** tab and select **Use Active Directory**.
2. Provide the following parameters:
    - **Domain name**: Domain name of the Active Directory.
    - **User name**: The user account used for querying the Active Directory.

      NOTE: The user account must have the read permission to query the Active Directory.
    - **Password**: Password of the account used for querying the Active Directory.
    - **Base DN**: Point from where the server searches for users. 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. Users not belonging to the specified Base DN will not be found in Active Directory during authentication. Hence, the authentication will not happen.
    - **Use SSL**: Option to enable LDAP over SSL for communicating with Active Directory server.
    - **Perform Primary Authentication**: This enables the user to perform primary authentication via Active Directory before an authentication happens via Starling Two-Factor Authentication.
    - **Advanced Settings**: This allows the user to modify the Active Directory attribute mapping. 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 **samAccountName** attribute in Active Directory.

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

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

Configuring user repository for CSV file

To configure the repository for data stored in CSV file:

1. Click the **User repository** tab and select **Use CSV file**.
2. Provide the path of the .csv file.

   NOTE: The order of the attributes in the CSV file must be UserName,PhoneNumber,EmailAddress.

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

Client configuration

You can configure the RADIUS clients by providing the client details in the **Client Settings** tab. You can add, remove or update IP address, subnet mask and shared secret of clients in the **Client Settings** tab.

Adding clients

To add client details:

1. Click the **Client Settings** tab.
2. Click **Add** and provide the following details:
   - **IP address**: IP address or the range of IP addresses from which Starling Two-Factor RADIUS Agent accepts authentication requests.
     For example,
     - 192.168.70.9: In this case, Starling Two-Factor RADIUS Agent allows authentication requests only from this IP address.
     - 192.168.70.0: In this case, Starling Two-Factor RADIUS Agent allows authentication requests from any IP address on the 192.168.70.0 subnet (Subnet mask 255.255.255.0 must be specified).
   - **Subnet mask**: This is an optional field. 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 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 Starling Two-Factor RADIUS Agent server and the RADIUS client.

Removing clients

To remove a client:

- On the **Client Settings** tab, select the client IP address or subnet mask and click **Remove**.

Updating clients

To update client details:

1. On the **Client Settings** tab, select the client and click **Update**.
2. Update the required details and click **OK**.

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

Configuring Starling Two-Factor RADIUS Agent in client application

To configure Starling Two-Factor RADIUS Agent in client application:

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

For more details regarding integration, see the client product documentation.

Logging into the client application

To log into the client application, you can use OTP or push notifications for two-factor authentication. The following are the scenarios that you will come across while generating OTP or push notifications.

NOTE: When you are logging into the client application for the first time, you will receive an SMS to install Starling 2FA app during two-factor authentication, if:

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

NOTE: If Perform Primary Authentication check box is selected in the configuration tool, enter the AD user password in the required field. Once the password is validated against AD, perform any of the authentication methods listed below.

OTP through SMS

To generate OTP through SMS:

1. On the client application, enter **SMS** in the token response field and click **Enter**. You will receive an SMS.
2. Enter the OTP received through SMS, in the token response field of the client application and click **Enter** to log in.

OTP through phone call

To generate OTP through phone call:

1. On the client application, enter **Phone** in the token response field and click **Enter**. You will receive a phone call.
2. Enter the OTP received from the phone call, in the token response field of the client application and click **Enter** to log in.

OTP through Starling 2FA app

To generate OTP through Starling 2FA app:

- If you are a new user:
    1. On the client application, leave the token response field empty and click **Enter**.
        a. If you have installed Starling 2FA app, then your token will be added to Starling 2FA app.
        b. If you have not installed Starling 2FA app, install the app and register your phone number (Install the app either from the SMS you have received or from the app store). Your token will be added to Starling 2FA app.
    2. Enter the OTP from the token in Starling 2FA app, in the token response field and click **Enter** to log in.
- If you are an existing user:
    - Enter the OTP from the token in Starling 2FA app, in the token response field and click **Enter** to log in.

NOTE: Starling 2FA app can be used for two-factor authentication on Android, iOS and Chrome.

Push notifications in Starling 2FA app

To use push notifications:

NOTE: To use push notifications you must install Starling 2FA app and register your phone number.

1. If you have not installed Starling 2FA app, install the app from the app store.
2. On the client application, enter **Push** in the token response field and click **Enter**. Your token will be added to Starling 2FA app.

3. Open Starling 2FA app and go to **OneTouch** menu.
4. Approve the request in the **Pending** tab to log in to the client application.

5

Diagnostic logging

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

Enabling diagnostic logging

To enable diagnostic logging for Starling Two-Factor RADIUS Agent:

1. On a computer where Starling Two-Factor RADIUS Agent is installed, go to the **Starling Two-Factor RADIUS Agent** folder in the installation directory. Normally, the path to the folder is **%ProgramFiles%\One Identity\Starling Two-Factor RADIUS Agent**.
2. Make the following changes to the **StarlingTwoFactor.RadiusAgent.Service.exe.config** file in the **Starling Two-Factor RADIUS Agent** folder:

- In the **<log4net debug="false">** entry, set the value to **"true": <log4net debug="true">**
- In the **<level value="ERROR" />** entry, set the value to **"DEBUG": <level value="DEBUG" />**

You can find the log file **RadiusAgent.log** in the Logs folder in the installation directory. Normally, the path to the log file is **%ProgramFiles%\ One Identity\Starling Two-Factor RADIUS Agent\Logs**.

Disabling diagnostic logging

To disable diagnostic logging for Starling Two-Factor RADIUS Agent:

- Set the following values in the **StarlingTwoFactor.RadiusAgent.Service.exe.config** file:
  - **<log4net debug="false">**
  - **<level value="ERROR" />**

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 or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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