One Identity Starling Two-Factor Desktop Login 1.0

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 Desktop Login Administration Guide
Updated - November 2018
Version - 1.0

Contents

1

Overview

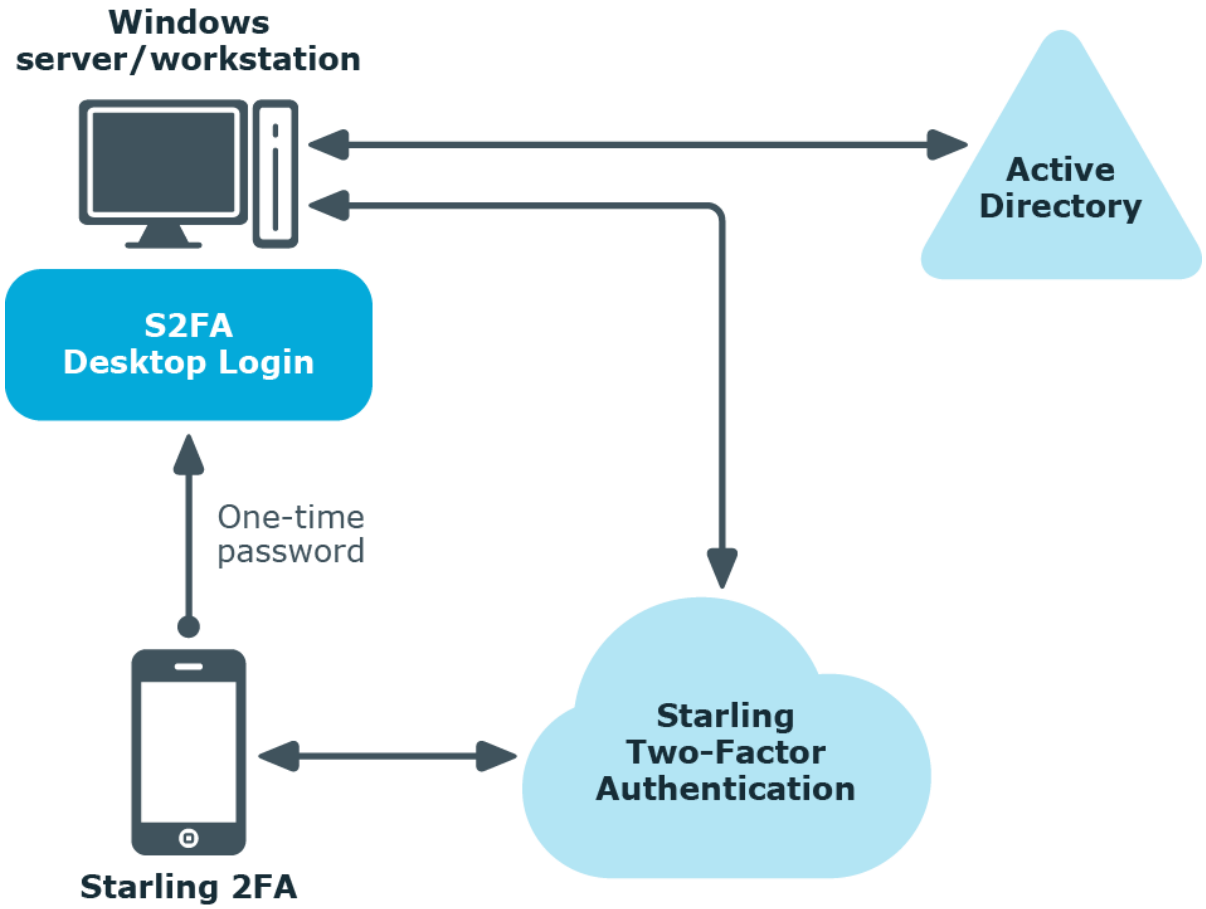
One Identity Starling Two-Factor Desktop Login offers companies and organizations the ability to add strong Two-Factor Authentication to Microsoft's Windows client and server operating systems. It provides a simple and consistent login experience, even when the user logs in to a local or terminal session. Starling Two-Factor Desktop Login ensures secured identity authentication by requiring user to approve push notification on Starling 2FA app or provide their Starling Two-Factor one-time password during the login process.

2

Deployment overview

One Identity Starling Two-Factor Desktop Login adds Two-Factor Authentication to all Windows login attempts. Use Starling Two-Factor Desktop Login to enhance typical Windows Login functions by adding a Two-Factor Authentication requirement to the username and password validation. Starling Two-Factor Desktop Login supports usage of **Login and Unlock Windows functions**.

Figure 1: Deployment overview



Connectivity requirements

Starling Two-Factor Desktop Login communicates with Starling Two-Factor Authentication using HTTPS. As the IP addresses can change over time, you must not lock down the firewall to an individual IP address.

Installation of Desktop Login

One Identity Starling Two-Factor Desktop Login supports both client and server operating systems.

Prerequisites

Before installing Starling Two-Factor Desktop Login on the computer, verify the following:

- Microsoft .NET Framework 4.5.2 or later is installed.
- Starling Two-Factor Authentication subscription is available and active.
- The computer is joined to an Active Directory domain.
- The computer on which Starling Two-Factor Desktop Login is installed, has network access.

Running the installer

Ensure that the caution detailed below is thoroughly read and followed before installing One Identity Starling Two-Factor Desktop Login.

CAUTION: After the installation is complete, the user must configure Starling Two-Factor Desktop Login settings to log in to the system.

To run the installer:

Double-click the appropriate installer, based on 32-bit or 64-bit platform and follow the instructions on the installer screens to complete the installation.

4

Starling Two-Factor Desktop Login Configuration

After installation, the One Identity Starling Two-Factor Desktop Login Configuration utility starts by default. The user can also start the utility from the **Start** menu. There are four tiles in the **Home** window. Each tile represents a configuration that must be done before using the product. Click **Manage Settings** to navigate to the required window and perform the following:

- Connecting with Starling for Authentication
- Configuring Push Notifications
- Configuring Active Directory Attributes
- Configuring Log On Settings

Connecting with Starling for Authentication

Starling Two-Factor Desktop Login enhances the authentication of Windows login by using Starling Two-Factor Authentication. To use One Identity Starling Two-Factor Desktop Login, you must have a valid Starling Two-Factor Authentication subscription.

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 Desktop Login 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 **Log 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 to One Identity Starling Two-Factor Desktop Login **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 Desktop Login is uninstalled, details regarding the Starling Two-Factor Desktop Login 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 account**. To test the validity of your account connection, click **Test connection**.

NOTE: If you have a Starling account, when a subscription is created for you, 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 Desktop Login must be joined.

NOTE: If you do not have a Starling account, when a subscription is created for you, 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*.

Configuring 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 2FA 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.

Configuring Active Directory Attributes

You can specify the user attributes that would be used to retrieve values of the log on user. In the **Active Directory** window, the config tool allows you to specify the user attributes that would be used to retrieve the user's email address and phone number from Active Directory. The following drop-down menus are available to specify the user attributes:

- E-Mail attribute (default attribute name - mail) - Select the attribute from the drop-down menu. By default, the following values are available as part of the drop-down menu:
  - mail
  - userPrincipalName
- Phone number attribute (default attribute name - mobile) - Select the attribute from the drop-down menu. By default, the following values are available as part of the drop-down menu:
  - mobile
  - homephone

  NOTE: The mobile phone number value must be in the *E.164* format.

The above mentioned user attributes can be used to retrieve the user's email address and phone number from the Active Directory.

NOTE: If the default attributes are not applicable to your organization, the user can customize the LDAP attributes using the **ConfigurationUtility.exe.config** file.

Select the **Enable LDAP over SSL** check box to communicate over secured LDAP connection with Active Directory server.

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

Configuring Log On Settings

This configuration enables segregation of users into those who must be authenticated or bypassed, by including or excluding a specific Active Directory group, during login to a computer.

NOTE: By default all domain users who log on to a computer that has Starling Two-Factor Authentication Desktop Login installed must authenticate via Starling Two-Factor Authentication. Local users will be unable to log on.

To configure authentication for the user groups, select one of the following options:

- **Require specified users log on using Starling Two-Factor authentication**: Specifies that the users in groups added to the **Groups list** must authenticate via

Starling Two-Factor Authentication when logging on to computers that have Starling Two-Factor Authentication Desktop Login installed. By default, this option is selected.

- **Allow specified users to bypass Starling Two-Factor authentication**: Specifies that the users in groups added to the **Groups list** do not have to authenticate via Starling Two-Factor Authentication when logging on to computers that have Starling Two-Factor Authentication Desktop Login installed.

Addition or Removal of Groups

To add groups into the list box, click **Add**. A **Select Group** dialog box displays. Select a group by entering relevant text in the text box. The added group's name and its path in the AD, gets reflected in the list box. To remove a group, click **Remove**.

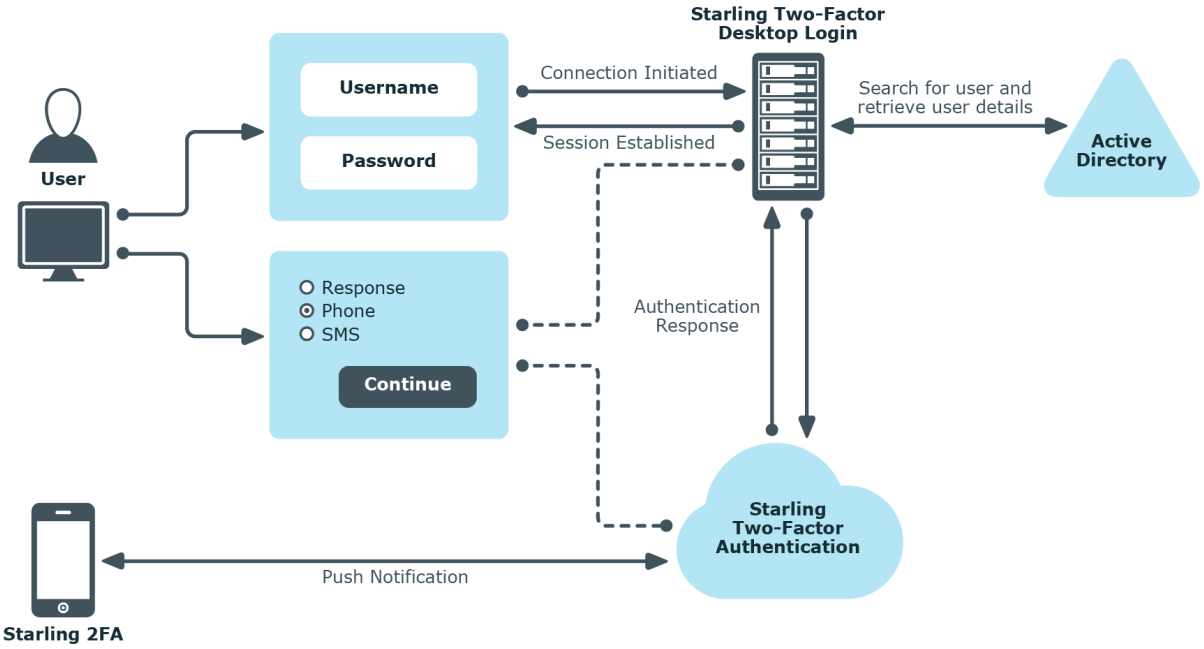
Unavailability of Starling Services

If the user is required to bypass Starling Two-Factor Authentication, when the Starling service is unavailable, select the **Allow users to bypass Starling Two-Factor authentication when Starling services are unavailable** checkbox. By default, the checkbox is unchecked and this setting does not permit the user to bypass Starling Two-Factor Authentication, when the Starling service is not available.

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

Network Diagram

Figure 2: Network Diagram: Starling Two-Factor Desktop Login



6

Test your setup

After the installation and configuration of Starling Two-Factor Desktop Login on the computer, log out and log in to the computer again.

Login to the system

When you log in to Windows locally or remotely with a valid Active Directory username and password, Starling Two-Factor Desktop Login sends a push notification to Starling 2FA app automatically after the primary authentication is successful. To use another method to log in, click **Sign in with another option** link from the **Verify Your Account** window. After clicking, the **Verify With A Token** window is displayed. Based on the option selected, the token response is provided through SMS, Phone Call or the Starling 2FA app.

NOTE: When you try to log in to the Starling Two-Factor Desktop Login application for the first time and if the Starling 2FA app is not installed, you will receive an SMS asking you to install the Starling 2FA app.

Use one of the following methods for Two-Factor Authentication.

Using push notifications

To receive a push notification, your phone number must be registered with your Starling account. You can approve or deny a push notification that is sent to your phone.

NOTE: If your phone does not receive a push notification, perform the following procedure:

1. Open Starling 2FA app and go to **OneTouch** menu.
2. Approve the request in the **Pending** tab to log in to the system.

Using OTP

OTP can be obtained through one of the following methods.

- OTP through SMS
- OTP through phone call

- OTP through Starling 2FA app

OTP through SMS

To generate OTP through SMS

1. On Starling Two-Factor Authentication **Verify With A Token** window, click **Text Message**. You will receive an OTP through SMS on the registered phone number.
2. Enter the received OTP in the token response field of the Starling Two-Factor Authentication **Verify With A Token** window, and click **Verify** to log in.

OTP through phone call

To generate OTP through phone call

1. On the Starling Two-Factor Authentication **Verify With A Token** window, click **Phone Call**. Your phone with the registered phone number will receive a call.
2. Enter the received OTP in the token response field of the Starling Two-Factor Authentication **Verify With A Token** window, and click **Verify** to log in.

OTP through Starling 2FA app

To generate OTP through Starling 2FA app

1. If you have installed the Starling 2FA app, your account is added to Starling 2FA app. If you have not installed the Starling 2FA app, install the app and register your phone number. Your account will be added to the Starling 2FA app.

   NOTE: Install the Starling 2FA app either by clicking the link in the SMS you have received or from the app store.

2. Enter the received OTP in the token response field of the Starling Two-Factor Authentication **Verify With A Token** window, and click **Verify** to log in.

NOTE: The Starling 2FA app is available on Android, iOS, and Google Chrome.

Diagnostic logging

To troubleshoot issues that may occur during authentication with Starling Two-Factor Authentication, enable diagnostic logging for Starling Two-Factor Desktop Login.

Enabling diagnostic logging

To enable diagnostic logging for Starling Two-Factor Desktop Login:

- On a computer where Starling Two-Factor Desktop Login is installed, create the following value in the

  HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Starling Two-Factor Desktop Login registry key using the Registry Editor:

  Value type: **REG_DWORD**

  Value name: **Diagnostics**

  Value data: **1**

The path to the log file: **%ProgramData%\One Identity\Starling Two-Factor Desktop Login\Diagnostics**

The filename for Starling Two-Factor Desktop Login Configuration tool log file: **Configuration.txt**

The filename for Starling Two-Factor Desktop Login logs: **2FA Desktop Login.txt**

Disabling diagnostic logging

To disable diagnostic logging for Starling Two-Factor Desktop Login:

Delete the Diagnostics value from the Starling Two-Factor Desktop Login registry key or set the value data to **0**.

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