



# Remote Assist

Administrator Guide



# Remote Assist – Administrator Guide

Securden provides secure remote access provisions for administrators and helpdesk technicians to troubleshoot devices remotely. Administrators can launch remote assist sessions through three different workflows.

| Remote Assist Mode       | Session Type  | Pre-requisite                                                                                                                                                                          | When to Use                                                                                                        |
|--------------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Attended Access</b>   | Agent Based   | 1. An active user must be present.<br>2. Agent must be installed on remote client.<br>3. Launcher must be installed on both remote client and host.                                    | Recommended for launching sessions on managed machines when users on active sessions need assistance.              |
| <b>Unattended Access</b> | Agent Based   | 1. Agent must be installed on remote client.<br>2. Launcher must be installed on both remote client and host.<br>3. Username and password of an account on the target machine.         | Recommended for launching sessions on managed machines for maintenance and troubleshooting outside business hours. |
| <b>On-demand Access</b>  | Browser Based | 1. An active user must be present on the remote device.<br>2. A browser must be installed on both remote client and host.<br>3. Connectivity between client and host must be possible. | Recommended for seamless one-time connections to machines without installing the agent.                            |

## Attended and Unattended Sessions

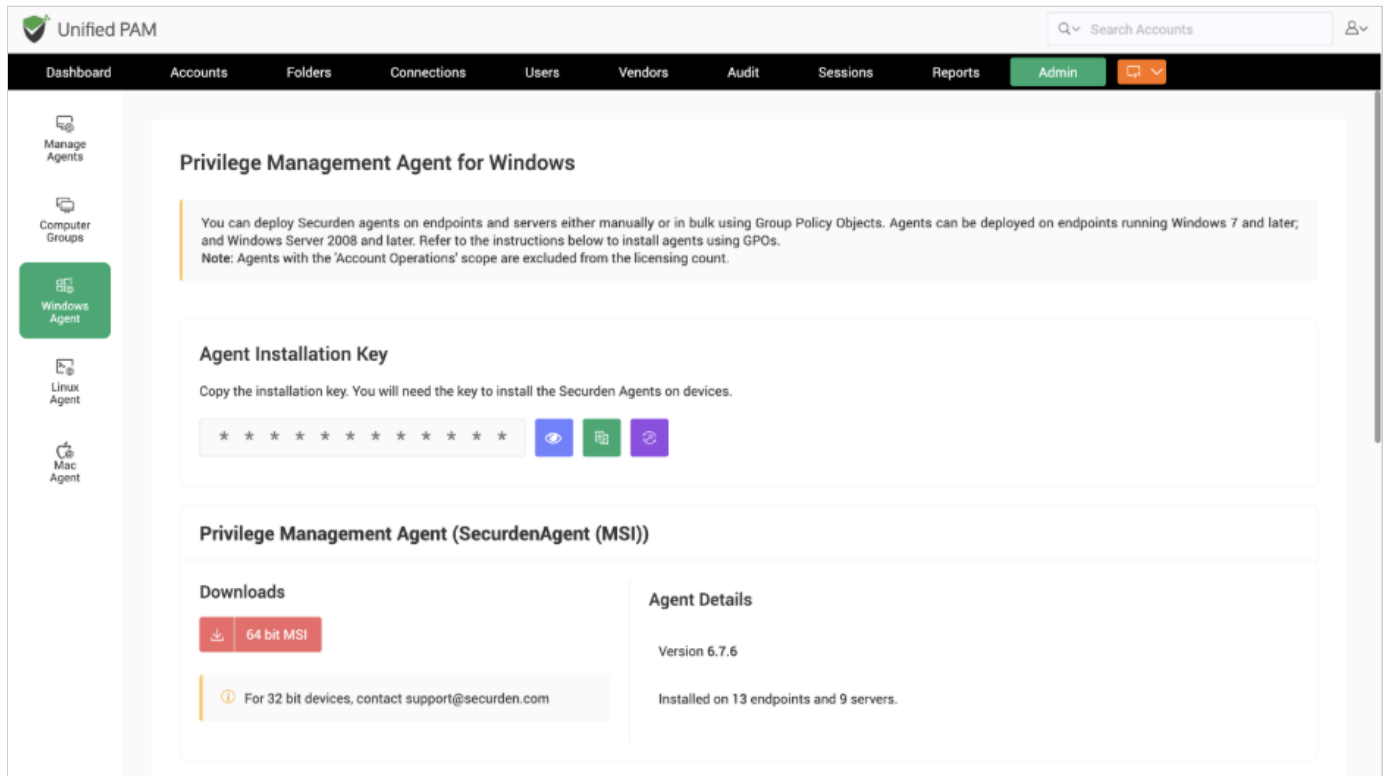
To launch agent-based attended and unattended remote assist sessions, you must follow the steps below.

1. Install the agent on both the remote client and remote host endpoints.
2. Create a remote assist policy and associate the policy with the technician and the required endpoints (remote client).

Once these steps are completed, technicians can start launching attended and unattended access sessions.

## Installing the Securden Agent on Endpoints

You must download and install the Securden agent available on the web-interface. You can start downloading the agent installer by navigating to **Admin >> Securden Agents >> Windows Agents**.



The screenshot shows the Securden Unified PAM web interface. The top navigation bar includes links for Dashboard, Accounts, Folders, Connections, Users, Vendors, Audit, Sessions, Reports, Admin, and a user profile icon. The left sidebar has icons for Manage Agents, Computer Groups, Windows Agent (highlighted), Linux Agent, and Mac Agent. The main content area is titled 'Privilege Management Agent for Windows' and contains the following information:

- Privilege Management Agent for Windows**  
You can deploy Securden agents on endpoints and servers either manually or in bulk using Group Policy Objects. Agents can be deployed on endpoints running Windows 7 and later, and Windows Server 2008 and later. Refer to the instructions below to install agents using GPOs.  
**Note:** Agents with the 'Account Operations' scope are excluded from the licensing count.
- Agent Installation Key**  
Copy the installation key. You will need the key to install the Securden Agents on devices.  
A field containing 16 asterisks and three icons (eye, copy, refresh).
- Privilege Management Agent (SecurdenAgent (MSI))**  

| Downloads                                        | Agent Details                            |
|--------------------------------------------------|------------------------------------------|
| <a href="#">Download</a> 64 bit MSI              | Version 6.7.6                            |
| For 32 bit devices, contact support@securden.com | Installed on 13 endpoints and 9 servers. |

**Important:** To install the Securden Agent, you must generate an installation key which must be provided at the time of installation. This is a one-time process. If you have already generated a key, you don't have to regenerate the key.

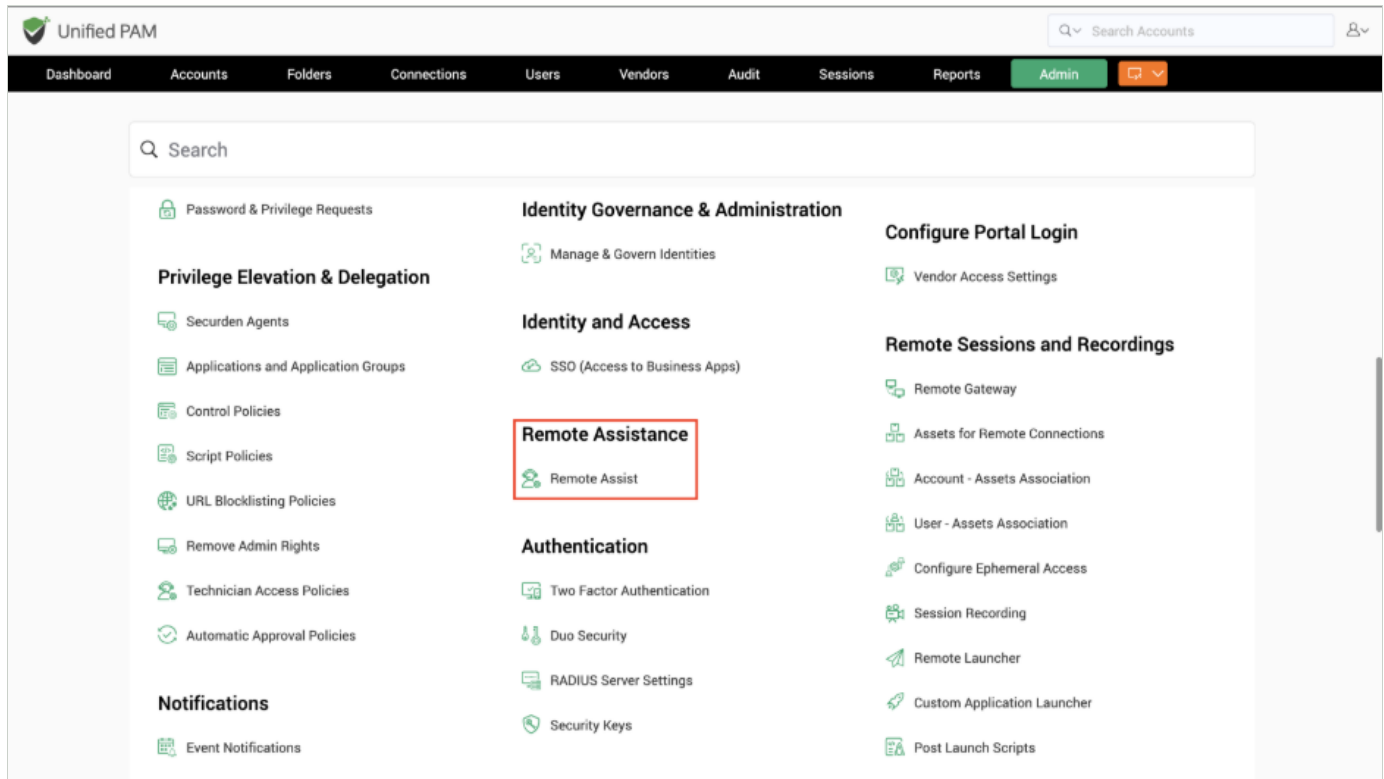
You may install the agent through methods listed below:

1. Direct installation on individual devices
2. Bulk deployment through:
  - a. Group Policy Objects (GPO) – refer [this document](#) for detailed steps.
  - b. Microsoft Configurations Manager – refer [this document](#) for detailed steps.
  - c. Any patch management tools like Intune, PDQ, etc.

# Creating a Remote Assist Policy

Securden Remote Assist works through policy-based access controls you can use to control which technicians are allowed to launch attended and unattended remote connections to specific devices.

For a technician to launch an agent-based remote assist session on an endpoint, a policy must exist allowing the technician to launch a session to that endpoint. You can create a remote assist policy by navigating to **Admin >> Remote Assist** and following the steps below.



1. In the Remote Assist module, go to **Policies** and select **Add Remote Assist Policy**.

Unified PAM

Dashboard Accounts Folders Connections Users Vendors Audit Sessions Reports Admin

On-Demand Assist  
Attended & Unattended Access  
Ongoing Sessions  
Session Archive  
**Policies**  
Audits

## Remote Assist Policies

You can create policies that govern which technicians are allowed to launch attended and unattended remote sessions to specific endpoints and servers.

Search Add Remote Assist Policy Delete Policies

| Name | Description | Type                    | Status           | Actions |
|------|-------------|-------------------------|------------------|---------|
| pol1 |             | Windows Computer Policy | Active [Disable] |         |

Showing 1 to 1 of 1 100

2. You must specify the **Policy Name** for this policy. You can optionally add a description to provide context for other administrators.

Unified PAM

Dashboard Accounts Folders Connections Users Vendors Audit Sessions Reports Admin

On-Demand Assist  
Attended & Unattended Access  
Ongoing Sessions  
Session Archive  
**Policies**  
Audits

## Create Remote Assist Policy

You can associate specific devices for technicians by creating suitable policies. Allow technicians to launch secure remote assist sessions for troubleshooting and maintenance.

Policy Name \* Description

**Associate Policy with Computers/Groups in Securden**

☒ All Windows Computers ☐ Specific Windows Computers/Groups

**Associate Policy with Remote Assist Users and Administrators**

☒ All Applicable Users  
☐ Include Specific Users/Groups  
☐ Exclude Specific Users/Groups

[Approval for Remote Assist Sessions?](#)

Save Cancel

### Help

Please refer to the section below for information regarding Technician Access Policies.

#### Remote Assist Policy Precedence

When multiple policies are associated with the same remote assist user, the assigned policy will be based on the following order of precedence.

All Applicable Users << Include Specific Users/Groups << Exclude Specific Users/Groups

#### Associate Policy with Computers/Groups in Securden

You can assign specific computers and computer groups for the remote assist technician or administrator by selecting the required computers/groups here. You can choose to associate all computers or choose specific computers and groups.

3. The next step is to associate the required remote computers with this policy. You can associate the policy with every computer managed using Securden or pick and choose specific computers and computer groups.

**Note:** The drop-down menu will only include the devices on which the agent is installed.

**Create Remote Assist Policy**

You can associate specific devices for technicians by creating suitable policies. Allow technicians to launch secure remote assist sessions for troubleshooting and maintenance.

Policy Name \*  Description

**Associate Policy with Computers/Groups in Securdent**

☐ All Windows Computers ☒ Specific Windows Computers/Groups

Search

- DEEPAKTEST
- DESKTOP-4F4R4FS
- DESKTOP-DFTEQ5S
- Group 1
- IGATEST21FNW84

**Help**

Please refer to the section below for information regarding Technician Access Policies.

**Remote Assist Policy Precedence**

When multiple policies are associated with the same remote assist user, the assigned policy will be based on the following order of precedence.

All Applicable Users << Include Specific Users/Groups << Exclude Specific Users/Groups

**Associate Policy with Computers/Groups in Securdent**

You can assign specific computers and computer groups for the remote assist technician or administrator by selecting the required computers/groups here. You can choose to associate all computers or choose specific computers and groups.

- Once all the required computers are selected, you must choose which users must be associated with the policy. You can simply associate the policy with all applicable users, select a few users and user groups from the drop-down, and associate the policy with them, or specify a few users and groups to associate the policy with everyone else.

**Note:** The preferences you select here will apply only to users with the role of **Administrator** or any custom user role with the **Launch Agent Remote Assist** permission.

- You can choose to enforce a consent from the user before assisted remote sessions can be launched. Click **Approval for Remote Assist Sessions >> Edit** to configure consent requirements.
- You have the option to auto-approve all connections, basically taking the control away from the remote user or enforce consent every time an admin launches a connection. You can configure whether to assume consent and non-consent when the consent prompts timeout.

## Remote Assist Approval Settings

**Auto-approve all connections:** Remote Assist sessions are approved automatically. Technicians gain immediate access to the target machine without any consent prompt shown to the end user.

**Ask end user (Approve on timeout):** A consent prompt is displayed on the target machine when a technician initiates Remote Assist. If the end user does not respond within the configured timeout, access is automatically approved.

**Ask end user (Deny on timeout):** A consent prompt is displayed on the target machine when a technician initiates Remote Assist. If the end user does not respond within the configured timeout, access is automatically denied.

**Note:** The timeout value defines how long the system waits for the user's response before automatically approving or rejecting the session.

☒ Auto-approve all connections ☐ Ask end-user (Approve on timeout) ☐ Ask end-user (Deny on timeout)

Save

Cancel

7. Once all the policy attributes are selected, you may **Save** the policy.

## Launching Unattended and Attended Remote Access Sessions

**Pre-requisite:** The Securden Remote Launcher must be installed on both the client and host machines. If you initiate a remote session, the system will automatically prompt you to install the utility. Optionally, you may use the same method you used to deploy the Securden Agent to install the launcher on all the required endpoints pre-emptively.

Technicians and administrators have two different ways to launch agent-based remote assist sessions. They can launch sessions through their agent or directly from the web interface.

### Launching Sessions from the Web Interface

Admins with a remote assist policy can simply follow the steps below to launch a remote assist session.

Navigate to **Admin >> Remote Assist** and go to **Attended & Unattended Access**.

**On-Demand Assist**

You can create a temporary session URL using which the client can initiate the remote assist session. Technicians can join the session once initiated.

**Note:** The URL created will expire within 15 minutes, and the client must connect before it lapses. You can adjust this duration in the Configurations tab.

Client Email Address (Optional)

Reason (Optional)

Launch Session with Admin Rights ☐

**Start Now**

**Help**

**Administrator Access on Remote Devices:**

Technicians will need administrator rights on remote devices to install and update software, troubleshoot, and modify system settings.

1. Select - "Launch Session with Admin Rights"
2. Provide credentials for authentication manually or choose an account stored in Securden.

- The Ongoing Sessions Tab displays all the sessions in progress or yet-to-start. Multiple technicians can join these sessions by clicking on the launch icon in this table.
- The session launched in the past will be available in the Session History tab.

**Session Expiry :**

Once generated, the session URL expires after a set time limit, and the client must connect before it lapses. You can adjust this duration in the Configurations tab.

Here, you will see the computers to which you are allowed to launch remote sessions.

To launch an attended remote session, click on **Launch Remote Assist** and select **Attended Access**.

**All Computers**

DESKTOP-4F4R4FS **Launch Remote Assist**

Unattended Access

**Attended Access**

**Computer Details**

|                   |                         |
|-------------------|-------------------------|
| DNS               | DESKTOP-4F4R4FS         |
| Operating System  | Windows 10 Pro          |
| Computer ID       | 2000020367172           |
| Last Logged in by | AzureAD\TestingSecur... |

**Securden Agent Details**

|                     |                            |
|---------------------|----------------------------|
| Status              | Running                    |
| Mode                | Operating                  |
| Scope               | Privilege Management       |
| Version             | 6.6.9                      |
| Type                | Privilege Management Agent |
| Last Connected Time | 2026/09/17 18:34           |
| Agent Type          | Privilege Management Agent |

**More Details**

|                     |                                  |                        |                                                  |
|---------------------|----------------------------------|------------------------|--------------------------------------------------|
| Serial Number       | 5189-9658-4179-1433-4061-5707-83 | Processor              | 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHzx2 |
| Total RAM           | 1.24 GB                          | Processor Architecture | 64-bit                                           |
| Device Manufacturer | Microsoft Corporation            | BIOS Version           | Hyper-V UEFI Release v4.1                        |
| Model               | Virtual Machine                  | OS Language            | English (United States)                          |
| OS Build Number     | 19045                            | OS Version             | 10.0.19045                                       |

If the system has an active session, a remote session will be initiated. If consent is enforced, the session will be initiated after the user consents.

To launch an unattended remote session, click on **Launch Remote Assist** and select **Unattended Access**.

Unified PAM

Search Accounts

DashboardAccountsFoldersConnectionsUsersVendorsAuditSessionsReportsAdmin

On-Demand Assist

Attended & Unattended Access

Ongoing Sessions

Session Archive

Policies

Audits

All Computers

DEEPAKTEST  
Windows Server 2019 Standard Evaluation  
Non-domain Computers

DESKTOP-4F4R4FS  
Windows 10 Pro  
Non-domain Computers

DESKTOP-DFTEQ5S  
Windows 10 Enterprise Evaluation  
securdenUS.onmicrosoft.com

Guhan's Mac  
Darwin 25.4.0  
Mac Computers

IGATEST21FNW84  
Windows 11 Pro  
Securden-lab.com

Mac (2)  
Darwin 25.4.0

DESKTOP-4F4R4FS

Launch Remote Assist

Unattended Access

Attended Access

Computer Details

DNS  
DESKTOP-4F4R4FS

Operating System  
Windows 10 Pro

Computer ID  
2000020367172

Last Logged in by  
AzureAD\TestingSecur...

Securden Agent Details

Status  
Running

Mode  
Operating

Scope  
Privilege Management

Version  
6.6.9

Type  
Privilege Management Agent

Last Connected Time  
2026/09/17 18:34

Agent Type  
Privilege Management Agent

More Details

Serial Number  
5189-9658-4179-1433-4061-5707-83

Processor  
11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHzx2

Total RAM  
1.24 GB

Processor Architecture  
64-bit

Device Manufacturer  
Microsoft Corporation

BIOS Version  
Hyper-V UEFI Release v4.1

Model  
Virtual Machine

OS Language  
English (United States)

OS Build Number  
19045

OS Version  
10.0.19045

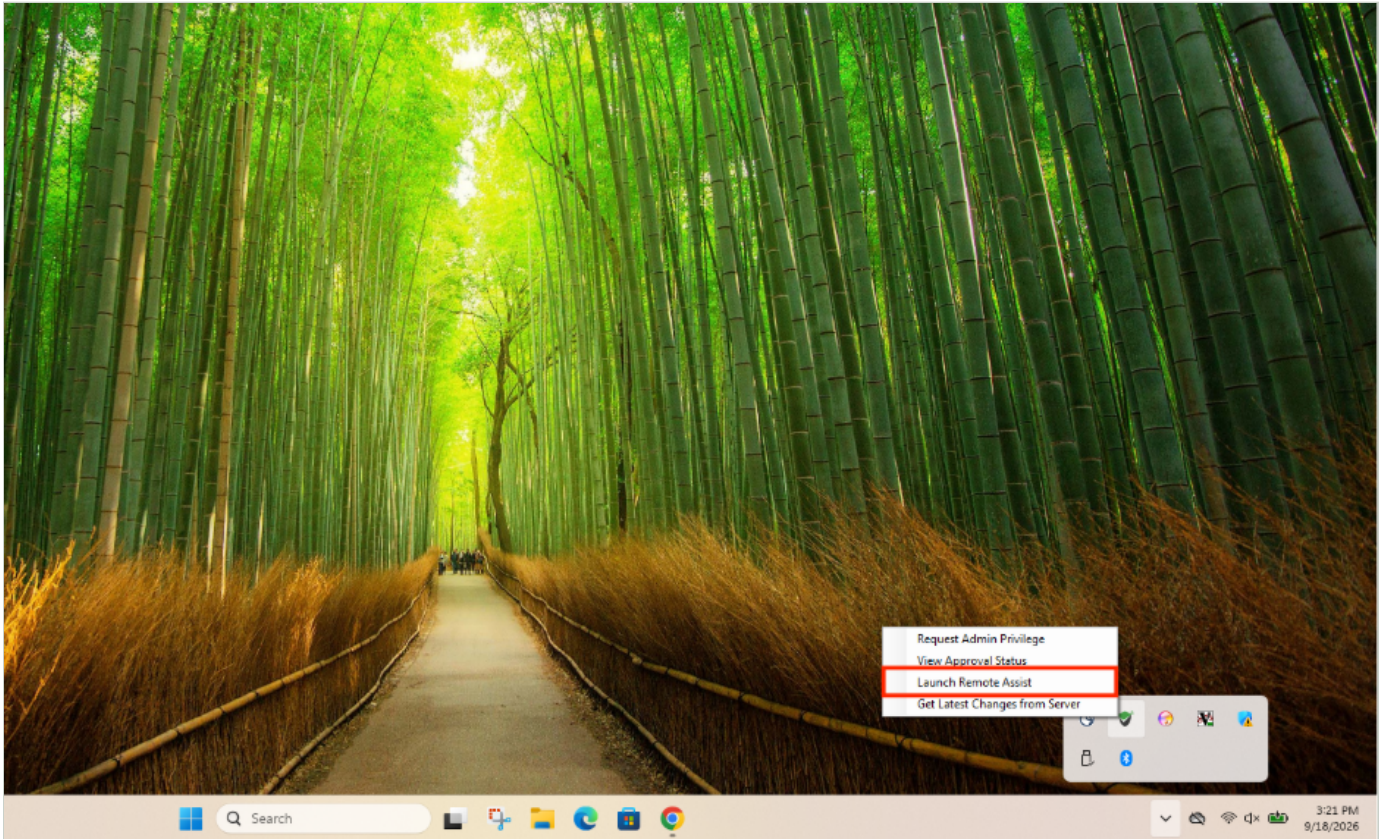
The session will be established immediately. You must login using the credentials of an account on the device manually.

### Launching Attended Sessions Using the Agent

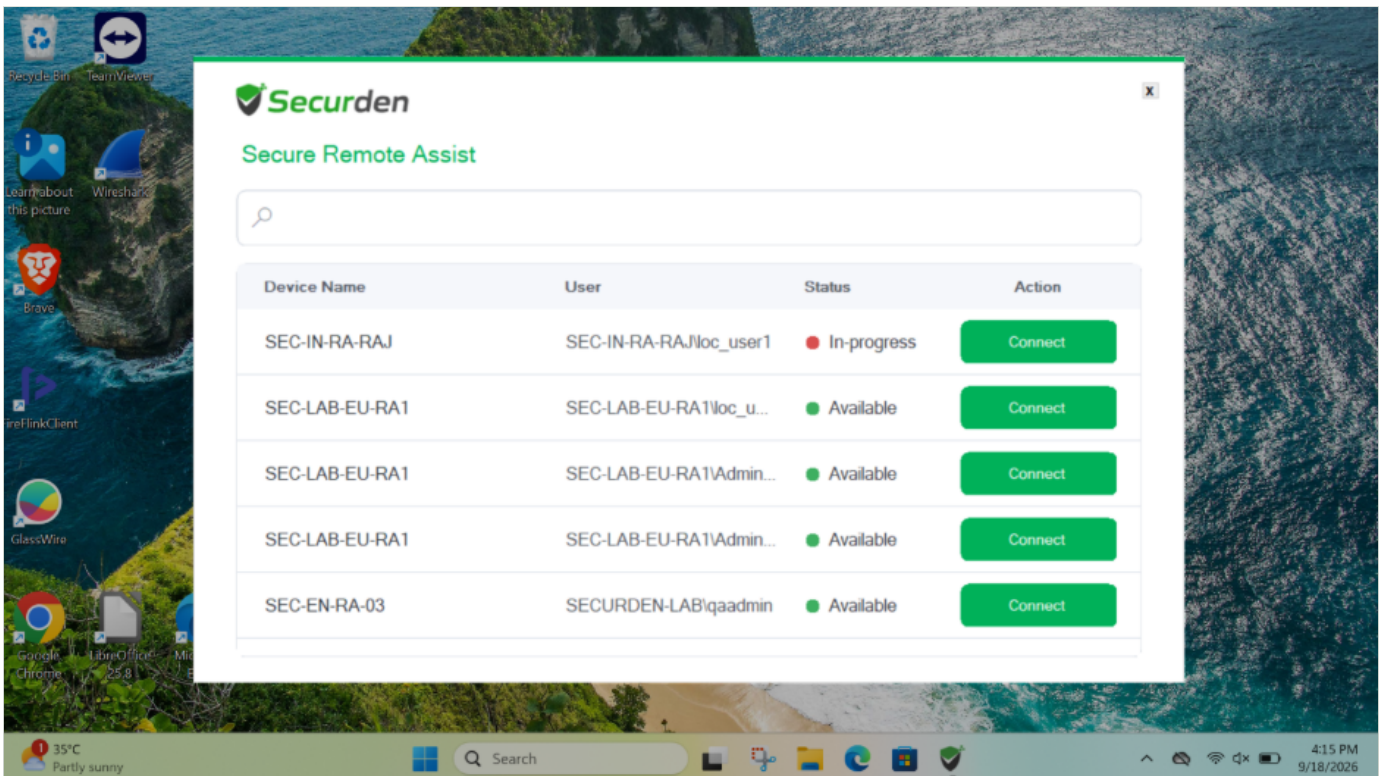
You can launch remote assist sessions directly using the Securden Agent.

Important: All sessions launched using agent are attended access sessions.

Technicians and Administrators with an active Remote Assist Policy can see the option to launch remote assist. Click **Launch Remote Assist**.

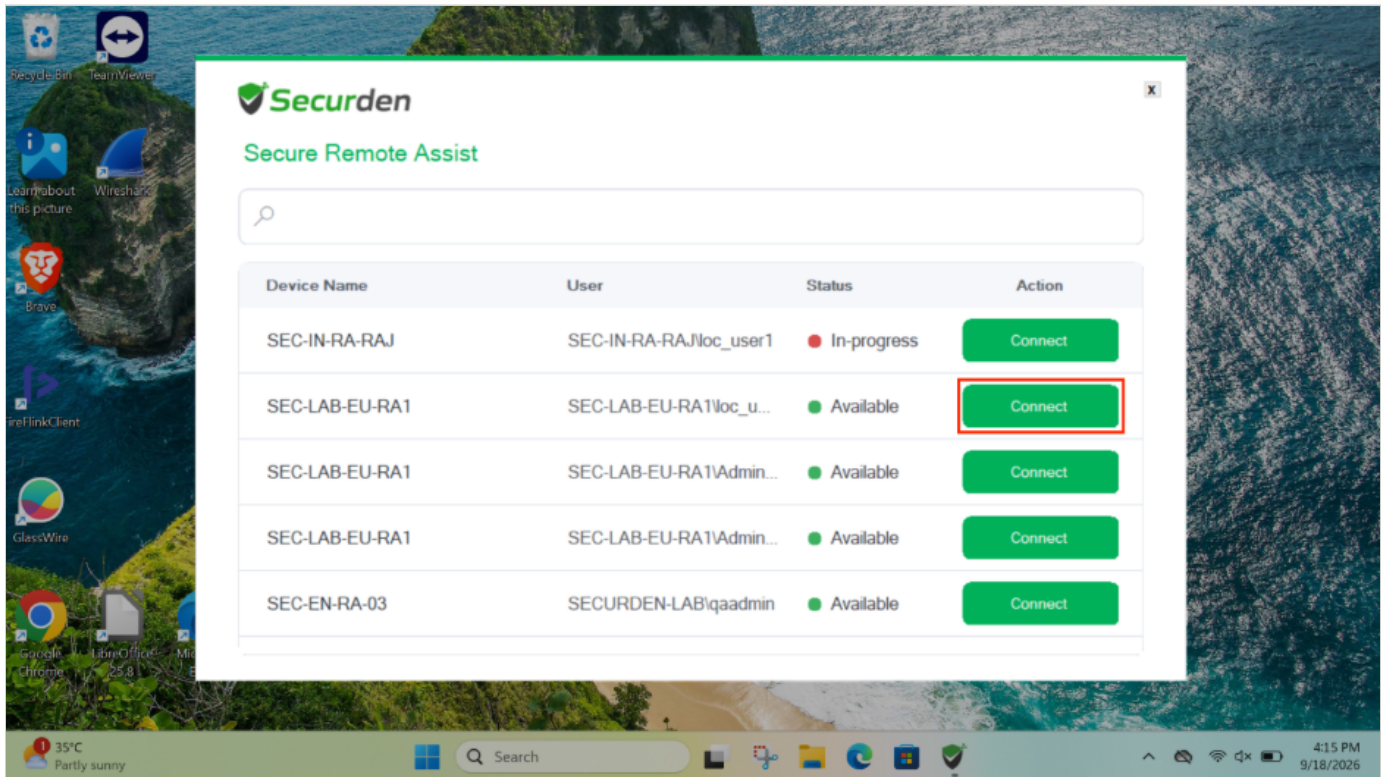


In the window that opens, you can see the devices to which you can launch remote sessions and the remote sessions that are currently going on. You can launch a new session to available devices or join active sessions.



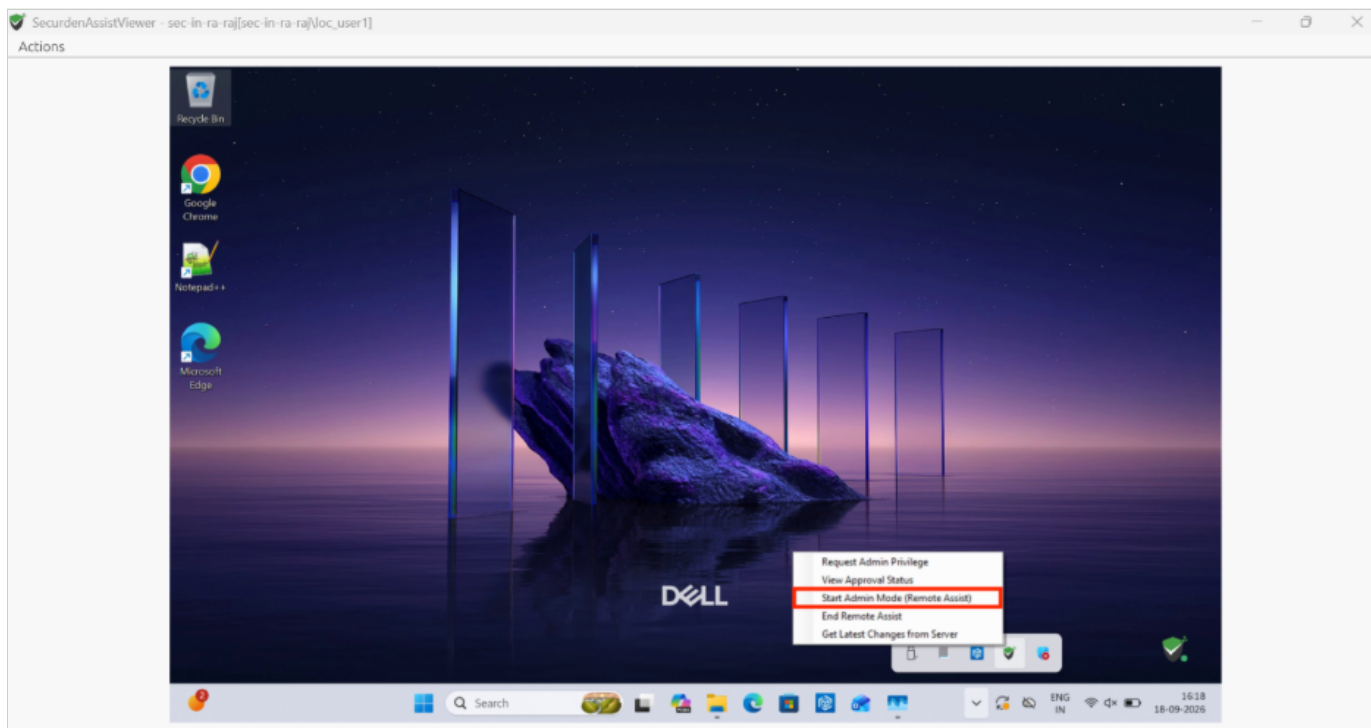
**Note:** Remote devices will only be listed here if they have the Securden Agent installed and running.

Click **Connect** to launch a remote assist session to a target device.



## Gaining Temporary Admin Privileges in Remote Assist Session

Once you have successfully launched a remote session, you can temporarily gain local admin privileges at the endpoint if required. Once you launch a remote assist session and connection is established, Click the Agent Tray icon on the **remote device** and select **Start Admin Mode (Remote Assist)**.



Once the need for elevated privileges is over, you can stop admin mode using the agent tray icon. Even if the technician fails to submit admin access, the permissions granted will be automatically revoked when the session ends.

## On-demand Remote Assist

Administrators and helpdesk technicians need to connect to remote endpoints for installing new applications, updating existing ones, and for general troubleshooting. Securden allows you to instantly launch remote assist sessions to any endpoint in your organization through a one-time access link.

In this guide, we will explore the steps the technician must follow to launch a remote connection to endpoints.

**Pre-requisites:** If you are using the on-premises edition of Securden, the server sends the remote assist URL directly to the remote user via email. You must configure Mail Server Settings from the admin console to send the emails to the remote user. If you haven't configured the Mail server settings, follow the steps below.

1. Navigate to **Admin >> General >> Mail Server Settings**.
2. Choose between basic authentication and modern authentication. Basic authentication uses credential-based authentication for your SMTP server. Modern Auth lets you connect to your email service through API based authentication.

3. Provide the required details based on your selection and send a test email to verify your configuration.
4. Click **Save**.

Establishing an **On-Demand Remote Assist Session** is a three-step process.

Step 1: Admin generates the session URL

Step 2: User joins the remote session (covered separately in the user guide)

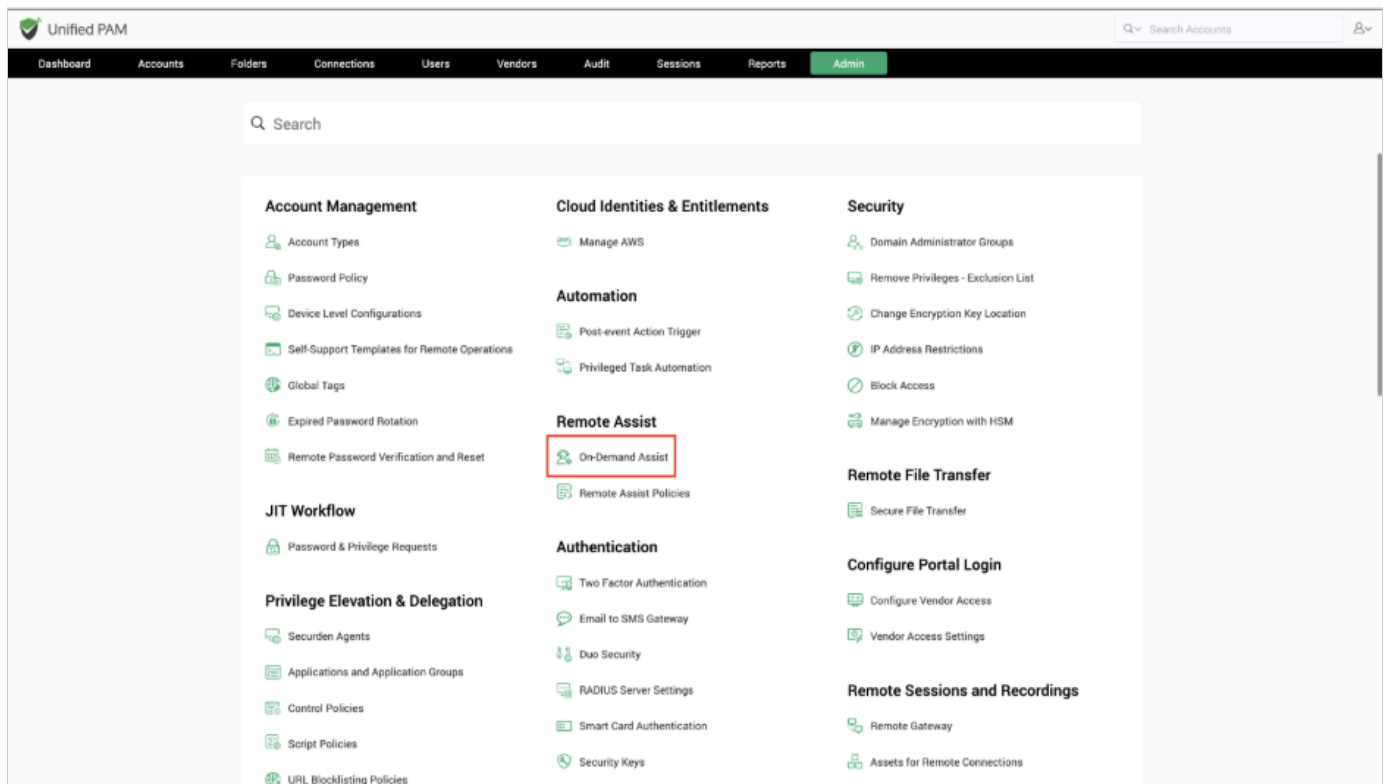
Step 3: Admin joins the active session

## Step 1: Generating the Session URL

Whenever a user needs help with installing/updating an application or with general troubleshooting, they will reach out to their IT admin or raise a helpdesk ticket. If the request requires the technician to log in remotely, they can launch an on-demand assist session in Securden to initiate secure remote access.

Follow the steps to generate the session URL:

- Navigate to **Admin >> Remote Assist >> On-Demand Assist Sessions**.



- Select **Create Session** from the left-hand menu.

**Unified PAM**

Search Accounts

Dashboard Accounts Folders Connections Users Vendors Audit Sessions Reports **Admin**

**Create Session**

Ongoing Sessions

Session Archive

### On-Demand Assist

You can create a temporary session URL using which the client can initiate the remote assist session. Technicians can join the session once initiated. The URL created will expire within 15 minutes, and the client must connect before it lapses. You can adjust this duration in the Configurations tab.

**Note:** The URL created will expire within 15 minutes, and the client must connect before it lapses. You can adjust this duration in the Configurations tab.

Session Name (Optional) Client Email Address (Optional)

Select Client Connection Tunnel (Optional) Reason (Optional)

☐ Launch Session with Admin Rights ⓘ

**Start Now**

### Help

**Administrator Access on Remote Devices:**

Technicians will need administrator rights on remote devices to install and update software, troubleshoot, and modify system settings.

1. Select the checkbox - "Launch Session with Admin Rights"
2. Provide credentials for authentication manually or choose an account stored in Securden.

- The Active Sessions Tab displays all the sessions in progress or yet-to-start. Multiple technicians can join these sessions by clicking on the session identifier in this table.
- The session launched in the past will be available in the Session History tab.

**Session Expiry :**

Once generated, the session URL expires after a set time limit, and the client must connect before it lapses. You can adjust this duration in the Configurations tab.

- Provide a suitable **Name** for the session. This is completely optional. By default, the date and time of the remote session are used as the session name.
- Specify the **Email Address** of the user on the remote machine. If you specify the email address, the session URL will be directly sent to the email recipient. However, this is completely optional. You can share the URL with the user directly through any method.
- You can optionally choose to route the session through a preferred gateway when connecting with users in a remote network. Select the preferred remote gateway from the drop-down.
- You can add a **Reason** for initiating the remote session for the record.

## Launch Session with Admin Rights

- If you require local administrator rights on the remote device, you must select the checkbox "**Launch Session with Admin Rights**".

**On-Demand Assist**

You can create a temporary session URL using which the client can initiate the remote assist session. Technicians can join the session once initiated. The URL created will expire within 15 minutes, and the client must connect before it lapses. You can adjust this duration in the Configurations tab.

Note: The URL created will expire within 15 minutes, and the client must connect before it lapses. You can adjust this duration in the Configurations tab.

Session Name (Optional)

Client Email Address (Optional)

Select Client Connection Tunnel (Optional)

Reason (Optional)

☒ Launch Session with Admin Rights ⓘ

**Supply Administrator Credentials ⓘ**

☒ Enter username and password ☐ Specify an account already stored in Securden

Username

Password

**Start Now**

**Help ⓘ**

**Administrator Access on Remote Devices:**

Technicians will need administrator rights on remote devices to install and update software, troubleshoot, and modify system settings.

1. Select the checkbox - "Launch Session with Admin Rights"
2. Provide credentials for authentication manually or choose an account stored in Securden.

- The Active Sessions Tab displays all the sessions in progress or yet-to-start. Multiple technicians can join these sessions by clicking on the session identifier in this table.
- The session launched in the past will be available in the Session History tab.

**Session Expiry :**

Once generated, the session URL expires after a set time limit, and the client must connect before it lapses. You can adjust this duration in the Configurations tab.

- You can explicitly provide the credentials of the local admin account or select an account stored in Securden. This account must have local admin privileges on the remote endpoint.

**On-Demand Assist**

You can create a temporary session URL using which the client can initiate the remote assist session. Technicians can join the session once initiated. The URL created will expire within 15 minutes, and the client must connect before it lapses. You can adjust this duration in the Configurations tab.

Note: The URL created will expire within 15 minutes, and the client must connect before it lapses. You can adjust this duration in the Configurations tab.

Session Name (Optional)

Client Email Address (Optional)

Select Client Connection Tunnel (Optional)

Reason (Optional)

☒ Launch Session with Admin Rights ⓘ

**Supply Administrator Credentials ⓘ**

☒ Enter username and password ☐ Specify an account already stored in Securden

Username

Password

**Start Now**

**Help ⓘ**

**Administrator Access on Remote Devices:**

Technicians will need administrator rights on remote devices to install and update software, troubleshoot, and modify system settings.

1. Select the checkbox - "Launch Session with Admin Rights"
2. Provide credentials for authentication manually or choose an account stored in Securden.

- The Active Sessions Tab displays all the sessions in progress or yet-to-start. Multiple technicians can join these sessions by clicking on the session identifier in this table.
- The session launched in the past will be available in the Session History tab.

**Session Expiry :**

Once generated, the session URL expires after a set time limit, and the client must connect before it lapses. You can adjust this duration in the Configurations tab.

Once completed, select **Start Now** to create the session URL. Once created, the URL will be displayed on a new tab as shown below.



## Secure Remote Assist

Secure assistance session

Share this Code or the Link with the end user to start remote assist

# 392-0380-078

<https://192.168.1.27:5959/join-remote-assist/392-0380-078>

Join Session

Copy Link

Waiting for user to connect...

Keep this page open. The session will start automatically once the launcher is opened by the end user.

Time remaining for user to join - 14:40

### Session Progress

- 1 Customer accessed the remote assist URL
- 2 Initiating Remote Assist Session
- 3 Connection established successfully

**Note:** You can simply click **Start Now** without specifying any details. The session URL will be created with the date and time of creation as the session name.

## Sharing the Session URL with Remote User

Once the session URL is created, you can copy the URL to your clipboard using **Copy Link** button and share the URL with the user on the remote endpoint. You can use a method of your choice for this purpose.



**Secure Remote Assist**  
Secure assistance session

Share this Code or the Link with the end user to start remote assist

**582-2633-263**

<https://192.168.1.27:5959/join-remote-assist/582-2633-263>

Join Session

Copy Link

**Waiting for user to connect...**

Keep this page open. The session will start automatically once the launcher is opened by the end user.

Time remaining for user to join - 14:52

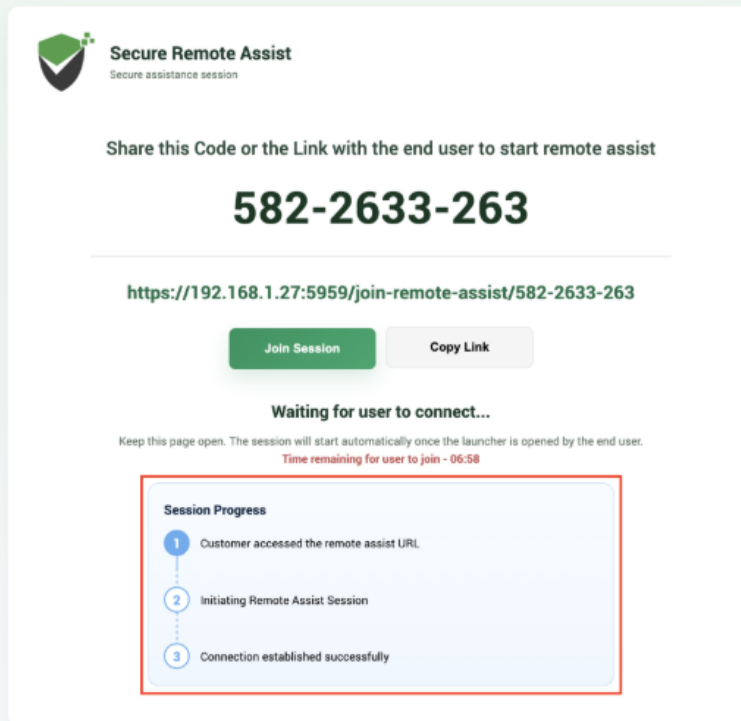
**Session Progress**

- 1 Customer accessed the remote assist URL
- 2 Initiating Remote Assist Session
- 3 Connection established successfully

**Note:** This URL is valid only for a limited time. The user must join the session within this time.

## Step 2: Wait for the User to Join the Remote Assist Session

Once the user receives the session URL, they have to go through a few steps to join the remote session. These steps are covered separately in the user guide.

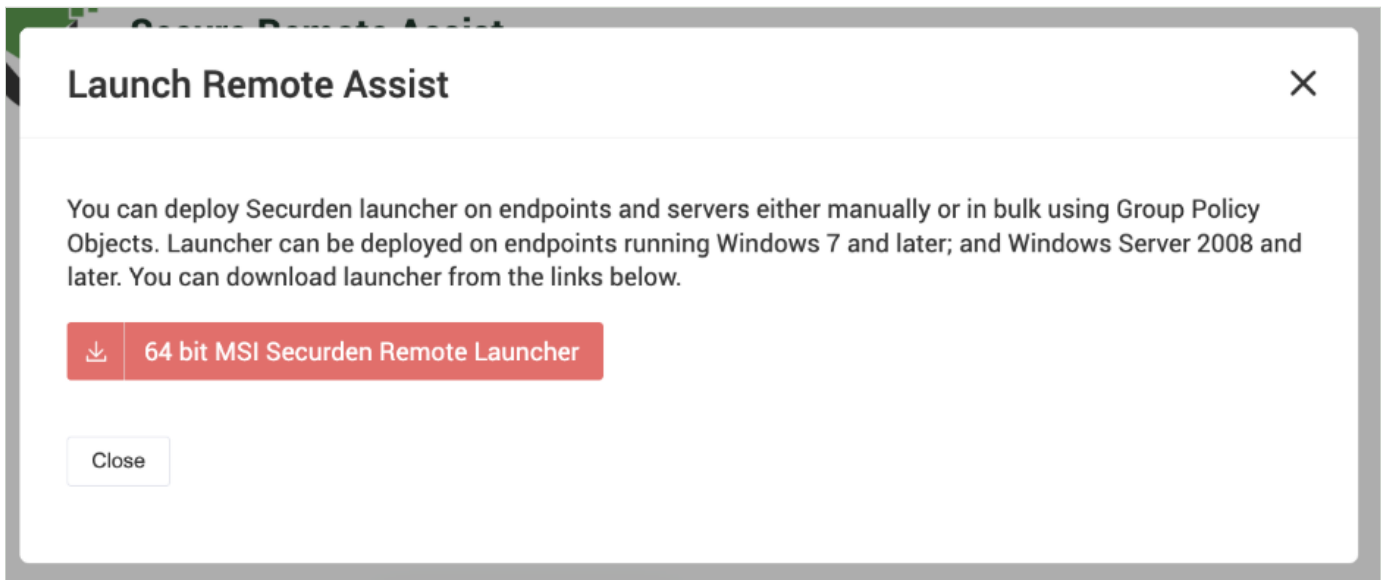


- Once the user opens the shared URL, the session progress will provide updates.
- Once the status changes to “Connection established successfully”, you can join the session. The steps are explained below.

## Step 3: Join the Remote Session

After the user starts the session, you can join the session by clicking on **Join Session**.

**Pre-requisite:** The Securden Remote Launcher must be installed to join any active remote assist session. If you try to join a session without the launcher, you will be prompted to download and install the software. You can download the installer from the pop-up as shown below.



After installing the launcher, you will be able to join the remote assist session by clicking on **Join Session** again.

## Collaborate with Multiple Technicians

Multiple technicians can join a remote assist session to collaborate and troubleshoot effectively. Technicians can join an active session by following the steps below.

1. In the Securden web-interface, navigate **Admin >> Remote Assist >> On-demand Assist**.
2. Here, go to **Ongoing Sessions**. The list of active sessions will be displayed in the table.

Unified PAM

Search Accounts

Dashboard Accounts Folders Connections Users Vendors Audit Sessions Reports Admin

Create Session

Ongoing Sessions

Session Archive

### Remote Assist Sessions

Active, ongoing, and about-to-start remote assist sessions are listed here.

Search Refresh Filter

| Session Title                 | Created By             | Created At        | Session Status       | Session Start time | Actions                                                                                                                                                                 |
|-------------------------------|------------------------|-------------------|----------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote Assist Session 17 J... | Securden Administrator | 17 Jun 2026 20:23 | Waiting for End User |                    |   |

Showing 1 to 1 of 1 25

<< < 1 > >>

3. Identify the required session by the session name and Click **Join Session** under the **Actions** column to join the session.

Unified PAM

Search Accounts

Dashboard Accounts Folders Connections Users Vendors Audit Sessions Reports Admin

Create Session

Ongoing Sessions

Session Archive

### Remote Assist Sessions

Active, ongoing, and about-to-start remote assist sessions are listed here.

Search Refresh Filter

| Session Title                 | Created By             | Created At        | Session Status       | Session Start time | Actions                                                                                                                                                                     |
|-------------------------------|------------------------|-------------------|----------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote Assist Session 17 J... | Securden Administrator | 17 Jun 2026 20:23 | Waiting for End User |                    |   |

Showing 1 to 1 of 1 25

<< < 1 > >>

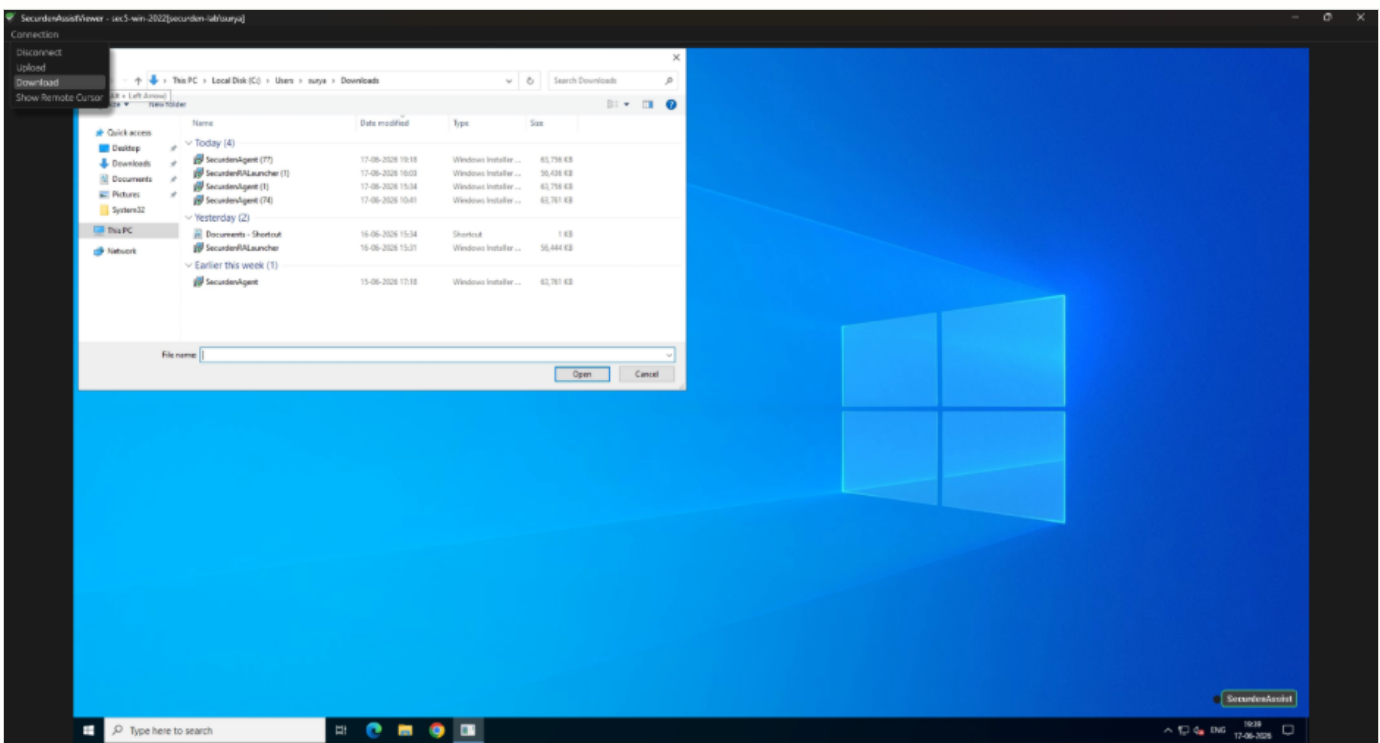
# Operations in an Active Remote Assist Sessions

Securden supports actions like transferring files between the connected devices and hiding the remote device pointer in the session.

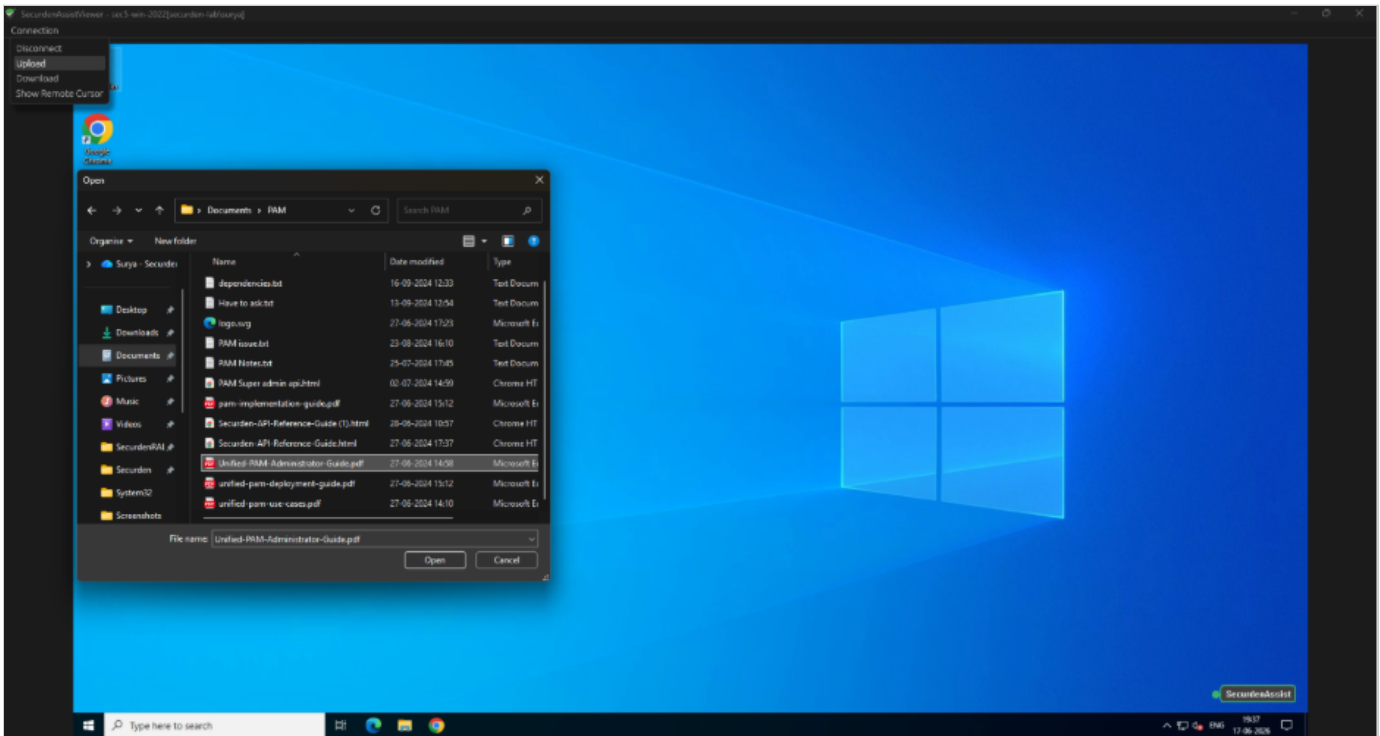
## Transferring Files from/to the Remote Device

During active remote assist sessions, technicians can transfer files from their machine to the remote machine and vice versa. This option allows the technician to export logs from the remote machine and push software installations seamlessly.

To transfer files from the technician's machine to the remote device, open the menu on top left corner and select "Download File". In the pop-up, select the file(s) required and proceed.



To transfer files to the technician's machine from the remote device, open the menu on top-left corner and select "Upload File". In the pop-up, select the file(s) required and proceed.



## Hiding the Remote User's Pointer

In the menu available in the top-left corner, you (technicians) can select “Show/Hide User's Pointer” to show and hide the remote user's pointer in the remote session.

# Closing a Remote Session

An active remote session can be terminated by the technician on the remote session, and any administrator or technician using the web interface.

1. Technicians on an active remote session can click **Disconnect** by using the menu available in the top-left corner of the assist screen to close the session.
2. From the web-interface, administrators and technicians can terminate open sessions by using the **Terminate Session Button** as shown below.

Unified PAM

Search Accounts

Dashboard Accounts Folders Connections Users Vendors Audit Sessions Reports Admin

Create Session

Ongoing Sessions

Session Archive

### Remote Assist Sessions

Active, ongoing, and about-to-start remote assist sessions are listed here.

Search Refresh Filter

| Session Title                 | Created By             | Created At        | Session Status       | Session Start time | Actions                                                                                                                                                                                                                                                     |
|-------------------------------|------------------------|-------------------|----------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote Assist Session 17 J... | Securden Administrator | 17 Jun 2026 20:20 | Waiting for End User |                    |    |

Showing 1 to 1 of 1 25

<< < 1 > >>

A confirmation pop-up will be displayed. You can click **Okay** and proceed to terminate the session.

## Session Recordings

All Remote Assist sessions are automatically recorded for auditing purposes.

You can view and replay these recordings at any time by navigating to **Sessions → Assist Session Recordings**

Q Search Accounts

Dashboard

Accounts

Folders

Connections

Users

Vendors

Audit

Sessions

Reports

Admin

Active Sessions

Recorded Sessions

Remote Assist Recordings

Remote Assist Recordings

Remote Assist sessions initiated by users can be recorded and securely stored for auditing and review purposes. You can playback recorded sessions at any time to monitor activities performed during the remote support session. The recordings help maintain accountability, support compliance requirements, and provide visibility into troubleshooting actions carried out by technicians.

Q Search

| Login Name                | Performed By | Start Time        | End Time          | Duration | Review & Playback |
|---------------------------|--------------|-------------------|-------------------|----------|-------------------|
| SECURDEN-LAB\surya        |              | 17 Jun 2026 19:52 | 17 Jun 2026 19:53 | 0:00:47  |                   |
| SEC_EN-EU-RA2\Surya-Admin |              | 17 Jun 2026 19:49 | 17 Jun 2026 19:51 | 0:01:54  |                   |
| SECURDEN-LAB\surya        |              | 17 Jun 2026 19:34 | 17 Jun 2026 19:50 | 0:15:53  |                   |
| SECURDEN-LAB\surya        |              | 17 Jun 2026 19:30 | 17 Jun 2026 19:32 | 0:01:45  |                   |

Showing 1 to 4 of 4

25

<<

<

1

>

>>

Here, click on the **Playback** button in the **Review & Playback** column against the required session.

Remote Assist

24