Sys-Manage

Passwordless Authentication for Workgroups

Administrator and User Guide

PIV smartcards and passkeys for local Windows accounts

Product version 1.9.4

Sys-Manage Informatica SL

Contents

For your first sign-in, start with chapter 1. Chapter 3 is for the administrator who assigns keys. Chapter 4 is for the person who uses them. To connect from another computer, follow the Remote Desktop instructions in chapter 5.

Introduction 3

1 Quick start 4

1.1 Set up a key and sign in 4
1.2 Choose the configuration language 4

2 Requirements and installation 5

2.1 Prepare the computer and account 5
2.2 Install the signed MSI 5
2.3 Upgrade an existing installation 6
2.4 Remove the product 6
2.5 View or activate the license 6

3 Administrator tasks 7

3.1 Create or assign a PIV key 7
3.2 Register a passkey 7
3.3 Identify multiple keys for an account 8
3.4 Remove a key assignment 8

4 User tasks 9

4.1 Set up data access for the first key 9
4.2 Set up data access for an additional key 9
4.3 Identify your key and read its status 10
4.4 Update an older passkey’s data access 10
4.5 Approve an administrator prompt 10

5 Local and remote sign-in 11

5.1 Sign in at the Windows console with a PIV smartcard 11
5.2 Sign in at the Windows console with a USB passkey 11
5.3 Prepare the client and target for Workgroup RDP 11
5.4 Set up certificate trust and the client connection 12
5.5 Sign in with NLA 13
5.6 Sign in without NLA 13

6 Troubleshooting and recovery 14

6.1 Recover from missing keys or unsuccessful registration 14
6.2 Resolve data access setup messages 14
6.3 Respond to a lost or unavailable key 15
6.4 Update access after a Windows password change 15
6.5 Collect logs for Sys-Manage Support 15

Introduction

Active Directory, Microsoft Entra ID and Linux already offer passwordless sign-in. When an organization adopts those options, local Windows accounts often remain the last accounts that still need a password. Examples include an operator account on a standalone workstation, a user account on a Windows server in a workgroup, and a local administrator account on a domain member server.

Sys-Manage Passwordless Authentication for Workgroups adds smartcard and passkey sign-in to an existing local Windows account. The computer continues to manage the account and its permissions. Users can sign in locally or through Remote Desktop.

PIV smartcards and passkeys

A PIV smartcard holds a private key and certificate. You can assign an existing certificate or create a new key on a compatible PIV device in the configuration app. The user enters the card PIN when prompted.

A passkey can be stored on a USB FIDO2 security key, an iPhone or an Android phone. During registration, choose the device in the Windows passkey dialog and confirm on that device. A USB key with both PIV and FIDO2 can be enrolled using either method.

Who sets up each key

The administrator assigns the key to the local account on the computer the user will sign in to. The user then opens the configuration app in their own account and selects **Set up data access**. That step lets the key sign the user in and keeps saved credentials available in their Windows session.

Chapter 1 walks through the first key. Chapter 5 shows where Windows asks for the card PIN or passkey when signing in locally or over Remote Desktop.

1 Quick start

Start on the computer that owns the local account. If you are setting up a key over Remote Desktop, enable device redirection on the client before connecting (section 5.3).

1.1 Set up a key and sign in

Prerequisites Install the product and restart Windows (section 2.2). Have a PIV smartcard, a USB FIDO2 security key, or an iPhone or Android phone for a passkey. An administrator makes the assignment. The account owner needs their Windows password and their device to finish setup.

1. As an administrator, open **Passwordless Authentication Configuration**. Select **Manage as administrator**, then **Users & Certificates → Add …**.
2. Select the account under **Local Windows user**. Check the name carefully if you are setting up a key for someone else.
3. Choose one of the following under **Key type / certificate**.

   Existing PIV certificate. Select the certificate and choose **Assign**.

   New PIV key. Connect only the intended PIV device. Select **Create a new key on a PIV device …**, then **Create & assign**. Follow the card prompts (section 3.1).

   Passkey. Choose **Register a passkey ...** and select **Register passkey**. Choose the USB key, iPhone or Android phone. If you choose a phone, make sure its Bluetooth is on. If Windows asks, select “Turn on Bluetooth” on the PC. Windows switches it off again afterward. Scan the QR code if shown. Confirm with the same device each time.
4. As the account owner, sign in with your Windows password. Open **Passwordless Authentication Configuration** in your own session.
5. Under **YOUR KEYS**, select the assigned key and choose **Set up data access**. Confirm with the device. When the selected key shows **Data access ready**, you can sign in with it.
6. Sign in with the key. At the computer, follow section 5.1 for PIV or 5.2 for a USB passkey. For Remote Desktop, open the prepared connection and follow section 5.5 or 5.6 according to its NLA setting.

Result Your Windows desktop opens under the enrolled local account.

1.2 Choose the configuration language

1. Select **Language …** (Sprache … or Idioma …) and choose **Windows default**, **English**, **Deutsch** or **Español**.
2. Close and reopen the app. Your preference also applies when you open the administrator view. Windows sign-in prompts follow the Windows display language.

2 Requirements and installation

2.1 Prepare the computer and account

Use the x64 installer on a 64-bit Windows workstation or server. A Remote Desktop destination also needs a Windows edition that can host the connection.

Prerequisites Have a local administrator who can install the product. If you administer the destination remotely, keep access to its local or virtual machine console while changing connection settings.

1. Choose an enabled local Windows account on the destination computer. For example, on a computer named WORKSHOP, enroll WORKSHOP\Alex. A domain account with the same user name is a different account.
2. For PIV, use a smartcard and reader that Windows recognizes. Use a card with an RSA certificate of at least 2048 bits or create a key on the card in section 3.1. For a passkey, have your USB FIDO2 key, iPhone or Android phone ready for the Windows dialog.
3. For Remote Desktop, install the product on the target (the computer that owns the account). If the target requires Network Level Authentication (NLA), install the same release on the client as well. With either setting, configure device redirection on the client before connecting (section 5.3).

2.2 Install the signed MSI

Prerequisites Obtain **PasswordlessAuth-Release-x64.msi** for this release from Sys-Manage. Schedule a restart and have local administrator credentials.

1. Right-click the MSI and open Properties → **Digital Signatures**. Select the Sys-Manage Informatica SL signature, then select Details. Verify that Windows reports **This digital signature is OK.** If a release hash accompanies the installer, compare it before running setup.
2. Open the MSI. Select I accept the terms in the License Agreement, then **Install**. Approve elevation for the per-machine installation. Select **Finish**.
3. Restart Windows. If the product is also installed on an RDP client, restart that computer after installation.

Result Open **Passwordless Authentication Configuration** from Start or the desktop. The desktop shortcut **Passwordless Authentication User Guide** opens the installed guide. Its file is located here:

```
%ProgramFiles%\PasskeyAuth\Documentation\PasswordlessAuth-User-Guide.pdf
```

If the installer reports that policy blocks custom LSA authentication packages, ask the Windows policy administrator to review the policy named in the message. If setup reports that rollback is disabled, have the Windows Installer policy reviewed before retrying.

Windows smart card sign-in. Setup leaves the built-in tile available for domain smart cards. To hide it deliberately, an administrator can edit the Windows policy **Computer Configuration → Administrative Templates → System → Logon → Exclude credential providers**. Add {8FD7E19C-3BF7-489B-A72C-846AB3678C96} to the exclusion list, keeping all existing entries. To show the tile again, remove only that ID.

2.3 Upgrade an existing installation

Prerequisites For an upgrade to a newer product version, have the signed MSI and access to a working Windows sign-in. Schedule a restart for each computer you update.

1. On the computer being updated, check the signature (section 2.2) and run the newer MSI as an administrator.
2. Restart Windows. For RDP with NLA, update both the client and the target to the same release.
3. Open **Settings → Apps → Installed apps** to see the installed product version. The personal configuration window also shows the version in its title.
4. Open the personal configuration window and select your usual key. If it shows **One-time update available**, follow section 4.4.

Corrected 1.9.4 installer. Use it for a new installation or an upgrade from an earlier version. During an upgrade, it removes the Windows smart card exclusion if the old installer recorded that it added it. To replace an installed 1.9.4 package, uninstall it first (section 2.4), then install the corrected package (section 2.2).

If you already run 1.9.4 and the Windows tile is visible, no action is needed. If the original installer hid the tile, an administrator can restore it without reinstalling. Remove only the ID in section 2.2 from ExcludedCredentialProviders under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System. Keep any exclusion required by your organization.

2.4 Remove the product

Prerequisites Before uninstalling, make sure each affected user can sign in with a Windows method that will still be available after removal. Have a separate administrator sign-in available.

1. On the computer to remove, open Settings → Apps → **Installed apps**. Find Sys-Manage Passwordless Authentication for Workgroups and choose **Uninstall**. Confirm and approve elevation.
2. Restart Windows. Users can then sign in with their remaining Windows sign-in options.
3. If you retire a Remote Desktop target, review the saved connection file and the listener certificate trusted by each client user (section 5.4).

Result The product and its guide are removed from this computer.

2.5 View or activate the license

The personal configuration window shows the license status at the bottom. For details or activation, select **Manage as administrator → About** and look under **License & activation**. Each computer on which the product is installed has its own license, including both endpoints when using NLA.

Select **Activate …** and follow the license dialog. After successful activation, **About** shows the license holder. After the 30-day trial expires, sign in with an available Windows method and activate the computer to resume PIV and passkey sign-in.

3 Administrator tasks

On the computer that owns the local account, open **Manage as administrator → Users & Certificates**. **Sign-in keys and user mappings** shows which key belongs to which local user. The account owner completes data access setup in the personal view.

If this computer is a domain controller acting as an RDP client, the administrator view offers **Logging** and **About**. Manage the destination's local account on the destination computer.

3.1 Create or assign a PIV key

Prerequisites Connect the PIV device and have its PIN ready. Over Remote Desktop, connect it to the client and enable smart card redirection (section 5.3). To create a key, connect only the intended device. An existing RSA key must be at least 2048 bits.

To create a key on a YubiKey, install the YubiKey Smart Card Minidriver on the computer running the configuration app. Use the standard driver for a direct USB connection or USB passthrough. For a card redirected over RDP, install the driver with Legacy Node (**INSTALL_LEGACY_NODE=1**) on the target.

1. In **Users & Certificates**, select **Add ….** Select the account under **Local Windows user**.
2. To use an existing certificate, select it under **Key type / certificate** and choose **Assign**.
3. To create a key on the connected device, select **Create a new key on a PIV device ….** Choose an RSA size supported by the card (2048, 3072 or 4096 bits). Set **Key requires touch** if wanted, then select **Create & assign**. Touch policy for an existing key is managed on the device.

Result Find the PIV entry next to the intended **Windows user**. The owner can now set up this key in section 4.1 or 4.2.

3.2 Register a passkey

Prerequisites Have the account owner's USB security key, iPhone or Android phone ready. Run the configuration app on the computer that owns the account. To register over RDP, enable WebAuthn redirection on the client before connecting (section 5.3).

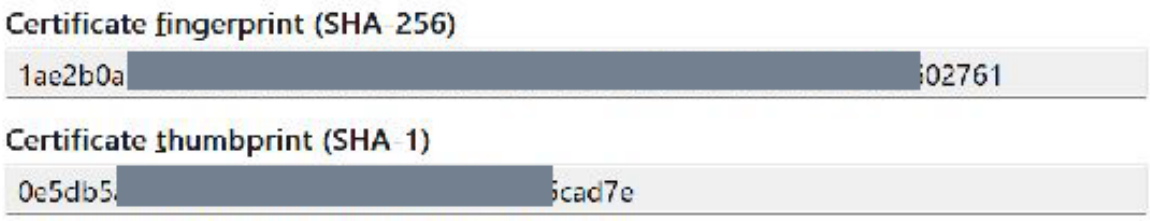
1. Select **Users & Certificates → Add … → Register a passkey ...** and choose the **Local Windows user**. In **Passkey name**, keep or edit the suggested name so the owner can recognize this registration later.
2. Select **Register passkey** and choose the device in the Windows dialog. Keep the phone near the PC (the client for RDP). If Bluetooth is off on the phone, turn it on in the phone's settings. Both devices need internet access. If Bluetooth is off on the PC, Windows may offer to turn it on temporarily. Accept the prompt and Windows will switch it off again when you finish. Scan the QR code if shown and confirm on the phone. If Windows asks again, choose the same passkey.
3. Wait for the app to report that the passkey was registered and check its row in **Sign-in keys and user mappings**. The account owner then chooses **Set up data access** for that passkey (chapter 4).

Result After renaming the target computer or changing its DNS suffix, register a passkey for the new name and set up its data access before using it for RDP.

3.3 Identify multiple keys for an account

Prerequisites Use the **Windows user** column to find the owner's entries. A user can have more than one key or passkey.

1. In **Users & Certificates**, find the rows for the account. To include a PIV card that is unplugged, select **Show saved mappings for disconnected PIV devices**.
2. For PIV, select **View …**. Compare **Certificate fingerprint (SHA-256)** with the value in the card tool, or **Certificate thumbprint (SHA-1)** with Windows. **Key ID (SHA-256)** identifies the public key and stays the same when a certificate is renewed on that key.
3. For a passkey, select **View …** to edit the displayed name. To distinguish two similarly named registrations, ask the owner to select each one in **Set up my hardware** and compare the full **Credential ID**. On a YubiKey, the corresponding value is in **Yubico Authenticator → Passkeys → Details**.



PIV key details with an example certificate. Both fingerprints are partially redacted.

3.4 Remove a key assignment

Prerequisites Before removing a key, make sure the owner can still sign in with the Windows password or another configured key. If you are replacing a key that still works, set up the replacement first.

1. In **Users & Certificates**, select the saved mapping. Check the account, key type, and key ID or fingerprint.
2. Select **Remove**, read the confirmation for this key and confirm. This removes the local assignment and its associated data access setup. The credential on the card, USB key or phone remains on the device.
3. If you enroll the same device again, the owner must set up data access again. For a lost device, follow section 6.3.

Result The removed key no longer appears under the account. Its other assigned keys are still available.

4 User tasks

Open **Passwordless Authentication Configuration** while signed in as the account owner. **Set up my hardware** shows your assigned keys. If you are using Remote Desktop, open the app on the target with device redirection enabled for your key (section 5.3).

4.1 Set up data access for the first key

Prerequisites An administrator has assigned the key to your local account. Have your Windows password and the device ready.

1. For your first key, sign in to the local account with your Windows password. If you are already signed in that way, continue in this session.
2. Open **Passwordless Authentication Configuration**. **Set up my hardware** shows the keys assigned to your account.
3. Under **YOUR KEYS**, select the key you want to use and choose **Set up data access**.
4. For PIV, follow the card PIN prompt. For a passkey, choose the passkey registered for this account and confirm on its device.

Result The selected key shows **Configured** and **Data access ready**. You can now sign in with that key using the appropriate method in chapter 5.

4.2 Set up data access for an additional key

Prerequisites An administrator has assigned the additional key to your account. Keep the device at hand.

1. Stay signed in to the account for which the new key was assigned. Open **Set up my hardware**. The app uses the data access available in this session to prepare the new key.
2. Under **YOUR KEYS**, select the additional key and choose **Set up data access**.
3. Confirm with the new key. If the app reports **Data access unavailable in this session**, follow section 6.2.

Result Select the new key and look for **Data access ready** before relying on it as your spare.

4.3 Identify your key and read its status

Prerequisites Open **Set up my hardware** in your own Windows session.

1. Select the PIV key under **YOUR KEYS**. If **Certificate SHA-256** is shown, compare it with the certificate in your smartcard tool. When the certificate is unavailable, **Key ID** identifies the public key instead.
2. For a passkey, compare the full **Credential ID** with the one shown by the authenticator when available. Two registrations can show the same account name.
3. Read the status for the selected key. **Not configured** means you still need to choose **Set up data access**. **Configured** and **Data access ready** mean you can use that key for sign-in.

4.4 Update an older passkey’s data access

Prerequisites Use this procedure if your passkey shows **One-time update available**. Have the same passkey and your current Windows password ready.

1. Sign in to the account with its current Windows password, as requested by the update message.
2. Open **Set up my hardware**. Under **YOUR KEYS**, select the passkey and choose **Update data access**.
3. Select the same passkey in the Windows prompt and confirm on its device.

Result The passkey shows **Configured** and **Data access ready**.

4.5 Approve an administrator prompt

When Windows asks for administrator credentials, open the available sign-in choices. If the prompt offers a **Smartcard** or **Passkey** entry for your local administrator account, select it and confirm with that account’s configured device. A standard user’s key by itself cannot grant administrator rights.

5 Local and remote sign-in

5.1 Sign in at the Windows console with a PIV smartcard

Prerequisites Connect the PIV device you set up for this local account in chapter 4.

1. Select the account or Other user. Under Sign-in options, choose the product's **Smartcard** tile for your local account. For a domain account, choose the Windows smart card tile (section 2.2).
2. At **Enter Smartcard PIN**, enter the card PIN and submit. Touch the device if the card policy requires it.

Result Windows opens your local desktop.

5.2 Sign in at the Windows console with a USB passkey

Prerequisites Connect the USB security key that holds the passkey you set up for this local account. Have its PIN ready if the device requires one.

1. At Windows sign-in, open **Sign-in options** if needed and select **Passkey** for the account.
2. Submit the **Passkey** tile. If **Enter security key PIN** appears, enter the USB key's PIN. Touch the key when it asks you to confirm.

Result Windows opens your local desktop.

5.3 Prepare the client and target for Workgroup RDP

Prerequisites Identify the target computer, the local account that will sign in and the client connecting to it. Keep a local or VM console available when changing the target's Remote Desktop settings.

1. On the target, open **Manage as administrator → Workgroup Remote Desktop**. Select **Enable Remote Desktop**, choose the **Network Level Authentication (NLA)** setting and select **Require TLS (recommended)**. Review the settings and confirm with **Apply** and **Yes**.
2. Turning Remote Desktop on or off here also updates its Windows Firewall exception. In Windows, give the account permission to sign in through Remote Desktop, for example through the target's **Remote Desktop Users** group.
3. Before connecting, configure redirection on the client. For PIV, select **Local Resources → More → Smart cards** or set **redirectsmartcards:i:1** in the .rdp file. For a passkey, set **redirectwebauthn:i:1** in that file. Target policy must allow the selected redirection. These settings let you create keys and set up data access in the session with or without NLA. Reconnect if you change them during a session.
4. If NLA is enabled, install the same product release on client and target. Assign the account's key on the target and have the owner set up data access there (chapters 3 and 4). With NLA, Windows asks for the credential on the client before opening the session (section 5.5). Without NLA, select the credential on the target's sign-in screen (section 5.6).

Result Use the target's computer name for passkey connections. It should resolve to the target and match its RDP certificate. Section 5.4 explains how to establish trust.

5 Local and remote sign-in

5.4 Set up certificate trust and the client connection

Prerequisites If Windows already trusts the target's listener certificate and it covers the connection name, connect using that name and continue with section 5.5 or 5.6. For a self-signed certificate managed with this product, use the following steps.

1. On the target, open **Workgroup Remote Desktop** and check the listener certificate and expiry date. If you need a new certificate, choose **Manage server certificate …**, enter the primary DNS name and any additional DNS names or IP addresses, then choose **Replace certificate**.
2. After replacing the certificate, check which certificate the target actually presents on a fresh RDP connection. If it still presents the old one, schedule a Remote Desktop service or computer restart and check again. **Restore previous** restores the saved binding if needed.
3. On the target, choose **Export client configuration …**. Enter the connection name covered by the certificate or leave the field blank for automatic selection. Save the JSON file. Transfer it to the client and confirm the certificate's SHA-256 fingerprint through a separate trusted channel.
4. On the client, open Windows PowerShell as the person who will connect. Use the JSON path and the independently confirmed fingerprint below. If the product is installed only on the target, obtain the matching **PasskeyRdpV1.ps1** from its administrator and use its actual path for **$tool**.

```
$tool = "$env:ProgramFiles\PasskeyAuth\PasskeyRdpV1.ps1"
$bundle = '<path to JSON>'
$expected = '<verified SHA-256>'
& $tool -Action Import -BundlePath $bundle -ExpectedSha256 $expected
```

After importing, find the **.rdp** file at the path printed after **Rdp=**. Check the redirection settings in that file (section 5.3), save it and use it to connect. When the target's certificate changes, repeat the export and import for affected users.

Result Import trusts the exported certificate for the current Windows user. Windows checks the target name and certificate trust when connecting. If an unexpected certificate appears, cancel and check the listener binding with the administrator.

5.5 Sign in with NLA

Prerequisites Both computers run the same product release. The local account has RDP permission and a configured key on the target. Prepare the client connection and its device redirection settings as described in section 5.3. If you use a phone, switch on its Bluetooth and keep it near the client PC. Allow Windows to turn on Bluetooth on the client if prompted.

1. Connect using the prepared **.rdp** file or the same settings in **Remote Desktop Connection**. Windows prompts for credentials on the client. Select **More choices** if you need to see the product's sign-in options.
2. For PIV, select the product's **Smartcard** entry for the exact certificate. Match its displayed identity to the assigned key. At **Enter the smartcard PIN for this certificate**, enter the PIN and complete any touch.
3. For a passkey, choose **Passkey**. In the Windows dialog, select the registered USB key or choose your phone if it is offered. Confirm with the device. Use the same passkey if Windows prompts again.

Result Your target desktop opens. Windows may reconnect you to an existing session for the account.

5.6 Sign in without NLA

Prerequisites NLA is disabled on the target. Prepare the client connection as described in section 5.3. You will select the credential at the target's Windows sign-in screen.

For a redirected YubiKey in PIV mode, install the YubiKey Smart Card Minidriver with Legacy Node (**INSTALL_LEGACY_NODE=1**) on the target. For a Hyper-V Enhanced Session, install it inside the guest VM.

1. Open the prepared connection for the target with NLA disabled (**enablecredsspsupport:i:0**).
2. For PIV, connect the card reader or USB device to the client. On the target sign-in screen, select the local account and **Smartcard**, then enter the card PIN and touch the device if requested.
3. For a passkey, select **Passkey** on the remote sign-in screen. In the Windows dialog on the client, choose the registered device and confirm. If you choose your phone, keep it near the client PC with Bluetooth enabled on the phone. Allow Windows to turn on Bluetooth on the client if prompted. The connection must support data access for that passkey.

Result The target desktop opens. If the sign-in screen cannot see your device, check the client profile and the target's redirection policy.

6 Troubleshooting and recovery

6.1 Recover from missing keys or unsuccessful registration

Prerequisites Use your Windows password or another configured key to reach the configuration app. Check the message for the key that failed.

1. If a PIV card or USB key is missing, check its connection. In an open setup window, select **Refresh** to rescan the key list. In **Users & Certificates**, you can also show saved mappings for disconnected PIV devices.
2. If an existing PIV certificate is missing from **Add sign-in key**, first check whether it is already in **Sign-in keys and user mappings**. If it is unassigned, check that Windows can read the card and that the certificate is valid and meets the RSA key-size requirement (section 3.1).
3. If a phone does not respond, check Bluetooth in the phone's settings and keep it near the PC. If a passkey was created on a device but the app did not finish registration, check the account's registration list before trying again. If Windows asks twice during registration, choose the same device and passkey both times.
4. If a key cannot sign in, have the owner check it in **Set up my hardware**. For **Not configured**, complete chapter 4. If only RDP fails, check the account's RDP rights, the connection name and the NLA setting. If the remote session cannot see the key, check client redirection and target policy (section 5.3).

PIN or device message. If asked to connect only one security key, unplug the other USB keys and retry. For an incorrect PIN, use the security key PIN. If Windows reports a blocked PIN, use another sign-in and follow the device provider's recovery procedure.

6.2 Resolve data access setup messages

Prerequisites Select the affected key in **Set up my hardware**. Use the message shown for that key.

1. **Finishing setup** — If this status persists after a short wait, select **Refresh** to read the current status. **One-time update available** — Follow section 4.4 using the same passkey.
2. **Data access unavailable in this session** — Sign in again with your current Windows password or a key that already provides data access, then retry. **Key not supported** — The key or its connection cannot complete data access setup. Use a different compatible passkey or PIV key.
3. **Data access recovery required** or **Data recovery required** — See section 6.4. Keep any session with access to the affected data available while the administrator investigates.

License status is unavailable. Use another Windows sign-in. Ask an administrator to check that **Passwordless Authentication Licensing** is running in Windows Services, then reopen **About**. If the trial has expired, follow section 2.5.

6.3 Respond to a lost or unavailable key

Prerequisites Have the current Windows password or another configured key. If the key was lost, notify the administrator responsible for each computer on which it was enrolled.

1. Use the account password or another configured key to sign in. If neither is available, contact the administrator before a password reset. A reset can affect access to previously encrypted data.
2. Have the administrator remove the lost key's assignment (section 3.4) on each affected computer. Follow your organization's lost-device procedure for the missing device. Assign the replacement to the account, then set up its data access in your own session.
3. Sign in with the replacement key using the console or RDP method in chapter 5.

Result The missing key's mapping is gone from the computer and you can sign in with its replacement.

6.4 Update access after a Windows password change

Prerequisites Read the message in **Set up my hardware** to distinguish an ordinary password change from an administrator reset.

1. If you change your Windows password normally, the product updates the data access information for your configured keys automatically.
2. For **Data access blocked** or **Data access recovery required**, use your current Windows password and contact your administrator. Additional keys can be set up once access is restored.
3. After an administrator resets the password, **Data recovery required** means that previously encrypted data needs separate recovery. Keep any session that still has access open. Contact the administrator about recovering the data from an available backup or recovery method.

6.5 Collect logs for Sys-Manage Support

Prerequisites Use the administrator view on the affected computer. For RDP issues, collect the time and the relevant messages on both client and target.

1. Select **Logging → Open text log**. If the log exists, it opens from C:\Windows\Temp\PasskeyAuth.log. Note the time of the problem so support can find the relevant entries.
2. Include the product and Windows versions, account type, device type, what you selected and the exact error. For RDP, include whether NLA was enabled and whether the failure occurred in the client prompt or on the target sign-in screen.

If support requests detailed tracing, use **Diagnostic level (ETW)** on **Logging**. Select the requested component and level, then **Apply**. The change takes effect when the affected process restarts. Tracing in LSASS requires a Windows restart. Record the original setting so you can restore it afterwards.

3. Redact account names, hostnames and unique IDs. Exclude passwords, PINs, private keys and protected data. Send the excerpt through your approved support channel to **support@sys-manage.com**.