imprivata®

Product Documentation

Imprivata Enterprise Access Management Best Practices

Imprivata Enterprise Access Management

Last Updated: January 2025

Contacting Imprivata

20 CityPoint, 480 Totten Pond Road, 6th Floor

Waltham, MA 02451 USA

Phone: 781-674-2700

Toll-Free: 1-877-OneSign

Fax: 1 781 674 2760

Support: 1 800 935 5958 (North America)

Support: 001 408-987-6072 (Outside North America)

https://www.imprivata.com

support@imprivata.com

Copyright and Legal Information

Trademark Information

Legal Notices

Document revision

Table of Contents

Imprivata Enterprise Access Management Security Considerations **4**
User Security Best Practices 4
Security Best Practices for Imprivata Administrators 4
Least Privilege and Limited Duration Access for Administrators 4
Administrator Roles and Delegated Administration 4
Two-Factor Authentication for Administrators 5
Administrator Password Management 5
Disabling an Administrator or Super Administrator Account 5
Security Best Practices for Imprivata End Users 6
Least Privilege and Limited Duration Access for End Users 6
Secure Remote Access 6
User Password and Imprivata PIN Management 6
Mobile Device Management for End Users 7
Two Factor Authentication for End Users 7
Disabling a User Account 7
Security Best Practices for Temporary Workers and Vendors 7
Imprivata Enterprise Access Management Environment Architecture Best Practices **9**
Environment 9
Certificates 9
Communication 10
Imprivata Appliances 10
Appliance Administrative Interfaces 10
Audit Records Management 11
Post to Syslog and Appliance Log Management 11
Configuring NTP 12
Setting Up SMTP and Appliance Notifications 12
Suspicious Email Alerts 12
Reduce Login Failure 12
Max bad attempts 12
Send Email Alert 12
Imprivata Admin Console Settings 12
Disable API Access 12
Procedure Code Extensions 13
Imprivata Admin Console Session Timeout 13
SPML Provisioning 13
Directories 13
Appliance Backup 13
Imprivata Agents 13
Imprivata Enterprise Access Management Authentication Best Practices **15**
Two Factor Authentication 15
Offline Authentication 15
Security Questions 15
User Challenges 15
User Lockout 16
Best Practices — Passwords 16
Best Practice — Default Passwords 16
Locking Workstations 16
Computer Policies Overriding User Policies 17
Imprivata Enterprise Access Management Single Sign On 17
Remote Access — Temporary Codes 18
Remote Access — Skip Second Factor 18
Revoke EPCS from a User 18

Imprivata Enterprise Access Management Security Considerations

User Security Best Practices

The sections below describe security best practices for Imprivata Enterprise Access Management administrators, end users, and temporary workers and vendors.

Security Best Practices for Imprivata Administrators

Least Privilege and Limited Duration Access for Administrators

A guiding principle for all user security is to limit the scope of access to only those who need it and to end that access for an individual or group when it is no longer needed. Imprivata strongly recommends an approach of **least privilege**, which for administrators means limiting them to only the operations, computers, or users that they must manage. For examples:

- Limit and record the names of users who have privileged access in the organization and the level of their access. Update the list whenever users with privileged access join or leave the organization.
- Restrict the number of administrators allowed to maintain multiple accounts for an application. For more information, see "Enabling Multiple Accounts for a Select Population" in the Imprivata Enterprise Access Management online help.
- Instruct administrators to log out of the Imprivata Admin Console and the Imprivata Appliance Console when they finish using those consoles for the present time. For more best practices for administrative consoles, see Appliance Administrative Interfaces.

Administrator Roles and Delegated Administration

Imprivata uses administrator and sub-administrator roles so you can delegate administrative authority throughout an enterprise. Imprivata provides three levels of administrator roles. One Super Administrator role can perform all operations in the enterprise. You can create as many subordinate roles as you need and have multiple users in each role.

The number of roles used typically depends on the size of your organization:

- **Small organizations** with only one or two IT department members do not need delegated administration. Those one or two administrators usually have Super Administrator privileges. Imprivata recommends having at least two people per site or region assigned to this role to avoid a scenario in which one leaves or does not have access to the other's credentials.
- **Mid-size organizations** might have, for example, two Super Administrators and four lower-level administrators. The four might be grouped into two pairs, with each pair having a different sub-set of privileges. For example, each pair might have limited access to properties, policy management, and/or user account management. Mid-size organizations often use a similar distribution of roles as large organizations, distributing roles to specific departments such as support, IT, or administration.

- **Large organizations** typically have multiple levels of administrators with more fully delegated administration of operations, user accounts, and/or geographic regions. Imprivata recommends placing five or six roles in an administrative group. Examples of administrator roles limited by operations may include Help Desk Administrator, Application Profile Creator, ID Token Administrator, and Compliance Auditor.

Imprivata Enterprise Access Management operational capabilities with the greatest importance for security and risk include:

- Assigning the Super Administrator role to a user, described in "Managing User Accounts" in the Imprivata Enterprise Access Management online help.
- Controlling access to the Imprivata Admin Console, which provides access to many critical operational capabilities. For more information, see "Imprivata Admin Console" in the help portal.
- Synchronizing the Imprivata users list to an active directory, described in "Synchronizing the Users List" in the online help portal. Synchronizing the Imprivata database updates the list of users in the Imprivata Admin Console to match the list of users in the selected directory server.
- Deleting a domain (directory), described in "Managing Domains (Directories)" in the help portal. When you delete an Imprivata domain, you delete all user records and all user application credentials for that domain.

For a comprehensive overview of administrator roles and capabilities, including delegated administration, see "Administrator Roles (Delegated Administration)" in the help portal.

Two-Factor Authentication for Administrators

If an extra layer of security is needed for certain users and/or computers, for example, for administrators or for access to virtual desktop servers, implement two-factor authentication by adding Imprivata ID for Windows access, and disable "password-only" access. When a user logs into Windows with their username and password, Imprivata ID sends a push notification to their mobile device. They accept and are granted access. For more details, see "Imprivata ID for Windows Access" in the Imprivata Enterprise Access Management online help.

Also see Two Factor Authentication.

Administrator Password Management

- Keep administrator passwords in a shared password safe, such as Dashlane, KeyPass, and so on.
- Whenever an IT employee leaves the organization, change key administrator passwords that day.
- Follow best practices for password complexity, as described in "Best Practice — Password Complexity" in the Imprivata Enterprise Access Management online help.

Disabling an Administrator or Super Administrator Account

To disable an administrator account, disable it first in the active directory and then also in Imprivata Enterprise Access Management. If you have automated synchronization between your Imprivata user list and active directory or directories, the next synchronization will disable the administrator account in OneSign. For better security, manually disable the account in EAM without waiting for the next

synchronization. Also change key administrator passwords across your organization, including for access to the Imprivata Admin Console and Imprivata Appliance Console.

If the account you are disabling is a Super Administrator account, then after you disable it in Active Directory, the synchronization with EAM will not disable the account in EAM. You must manually disable or delete the account from EAM. Also change key administrator passwords and Super Administrator passwords across your organization.

Security Best Practices for Imprivata End Users

Least Privilege and Limited Duration Access for End Users

- Ensure that users do not have administrator access to endpoint devices, including Windows administrator privileges and Linux root privileges. The Windows registry on Windows endpoints and the Imprivata folders on all endpoints should be protected from end-user access.
- Ensure that users cannot install applications themselves. All application folders should be protected by default.
- Deploy applications only to users who need those applications. If applications share credentials, then the application vendor must control and limit access to those applications. For applications that don't share credentials, you can limit the deployment of those applications to end users. In the latter case, disable access in the third-party application and also in EAM for layered security.
- Restrict the number of users allowed to maintain multiple accounts for an application. For more information, see "Enabling Multiple Application Accounts for a Select Population" in the Imprivata Enterprise Access Management online help.
- Use inactivity detection of less than 15 minutes in physical areas where users tend to use one workstation or remain in the area. Imprivata also recommends using Secure Walk Away, as described in Locking Workstations.

Secure Remote Access

- Provide a VPN to secure traffic for employees when they are offsite.
- Use Imprivata Enterprise Access Management Remote Access for users' remote access and enforce two factor authentication especially when accessing from offsite. For more details, see "Remote Access: Before You Begin" in the Imprivata Enterprise Access Management online help.

User Password and Imprivata PIN Management

- Imprivata Self-Service Password Reset provides a convenience feature for users that can reduce calls to your help desk. For full details, see "Imprivata Self-Service Password Reset" in the Imprivata Enterprise Access Management online help. Consider the various factors involved for greater or lesser security, including:
  - Requiring re-authentication after password reset.
  - Allowing remote/external access to Imprivata Self-Service Password Reset. If you allow this access, allow HTTPS traffic only to the URLs and ports specified in that topic. Do not allow POST

requests to any URL except the URL listed in the table in that section. For all other URLs, allow only GET requests.

  - For details on underlying security aspects of this feature, see "Technical Considerations" in that help topic.

- Similarly, Self-Service Reset lets users enter their password or answer security questions to reset a forgotten PIN. You can manage the security questions and require users to enroll security questions. For more details, see "Self-Service Imprivata PIN Reset" in the help portal.
- Regarding the Imprivata Password Manager, if some or all users do not need to view or manage their own credentials, then disable this password manager for those users. You can disable it for some or all users in user policies under the Single Sign-On tab, as described in "Configuring SSO in User Policy" in the help portal. For more details on this password manager, see "The Imprivata Password Manager" in the help portal.

Mobile Device Management for End Users

Instruct users to report lost, stolen, discarded, sold, recycled, or replaced mobile devices to your helpdesk within 24 hours. In such cases, delete the user's Imprivata ID enrollment as described in "Managing User Devices" in the Imprivata Enterprise Access Management help. After a device is replaced, the user must download the Imprivata ID app again and enroll a new Imprivata ID. You can also enable users to delete an enrolled Imprivata ID from their workstation without calling your helpdesk first. For related information, see "Temporary Codes for Windows Access" in the Imprivata Enterprise Access Management online help.

Two Factor Authentication for End Users

Require two-factor authentication and disable "password-only" authentication for end users. For additional details, see Two Factor Authentication.

Disabling a User Account

To disable a user account, disable it first in the Active Directory and then also in Imprivata Enterprise Access Management. If you have automated synchronization between your Imprivata user list and active directory or directories, and if that synchronization frequency is every hour, then the next hourly synchronization will disable the user account in Imprivata Enterprise Access Management.

For better security, and if your synchronization period is longer, manually disable the account in Imprivata Enterprise Access Management without waiting for the next synchronization.

Security Best Practices for Temporary Workers and Vendors

- For temporary workers for whom you want to provide Imprivata services but do not want to have regular network accounts, you can create an Imprivata Directory Domain from which you can create those user accounts. Imprivata recommends that you create one or more user policies for those new users. For details, see "Creating Imprivata Accounts for Non-Domain Users" in the Imprivata Enterprise Access Management online help.

  You also can implement a password change policy for an Imprivata Directory Domain, as described in "Implementing a Password Policy" in the help portal.

- Alternatively, temporary codes can be used when you need to provide Windows desktop two factor-authentication to a temporary user such as a contractor. The user uses their network password as their first factor and the temporary code as their second factor for authentication.
  - Temporary codes are only available for Imprivata Enterprise Access Management Remote Access and Imprivata ID for Windows Access.
  - Specify a temporary code expiration for when the worker no longer needs access. The maximum time period allowed is 14 days. Because this user will only ever authenticate with their password and a temporary code, place them in a user policy separate from your permanent employees.
  - Temporary contractors should not be allowed to enroll any authentication methods. For more information, see "Temporary Codes for Windows Access" in the help portal.
- Ensure that vendors who access the Imprivata system propose remote access periods. Enable their accounts only for the time period needed and set them to expire after that period.

Imprivata Enterprise Access Management Environment Architecture Best Practices

Imprivata understands the importance of data security to your organization. Much of the security is built into the Imprivata Enterprise Access Management product.

The Imprivata appliance is a closed, locked down system.

- The Imprivata appliance is accessible only through authenticated sessions in the Imprivata Appliance Console, by Imprivata Enterprise Access Management client software, or the appliance APIs (Confirm ID, Prove ID Web, and Prove ID Embedded).
- All unnecessary services on the appliances are closed and there is no command line access to the appliance.
- There is no direct operating system or database access.
- There is no ability to modify or create operating system or database users.
- Software updates can only be done through the Imprivata Appliance Console and only in the form of digitally signed packages from Imprivata.

With that understanding, there are several environment and configuration settings that directly impact the security of the Imprivata solution. This section outlines best practices related to the implementation of the Imprivata Enterprise Access Management solution.

Environment

The Imprivata appliance is designed with standalone security measures, but strong security practices involve a defense in depth approach. For defense in depth, the appliance relies on secure environments in which to operate:

- The Imprivata appliances must be hosted with appropriate physical data center security.
- The appliances rely on strong corporate network security. Appliances are meant to be internal, never Internet facing.
- The hypervisor infrastructure hosting the appliances must be secured, with only appropriate individuals having access to the infrastructure.

  For other security considerations for the hypervisor infrastructure, see the documentation from your hypervisor vendor.

Certificates

- Use TLS to secure communications, whenever possible. This is especially important in the following scenarios:
  - Establishing trust with an LDAP directory server.
  - Importing users from Active Directory. For more information, see "Managing Domains (Directories)" in the Imprivata Enterprise Access Management Online Help system.

- Use certificates from the Active Directory PKI infrastructure.
- On Linux thin clients, when configuring ProveID Embedded, install the Domain Root CA certificate.
- Track the certificates that are in use. Take special note of the following:
  - The expiry date of the certificates.
  - Where the certificates are installed or being used.

Communication

Consider the following items when configuring the communication to the Imprivata enterprise in your organization:

- Use firewall access rules for internal servers to external to communicate only with known and trusted DNS names.

  Use SSL inspection where this is able to be used (where SSL inspection will not cause communication issues)..
- Configure a separate VLAN for the server subnet, so that traffic such as broadcast traffic or port scans from the wider network have no effect.

Imprivata Appliances

Appliance Administrative Interfaces

There is no direct remote access to the Imprivata appliance via command line interfaces at the operating system or database level. There is access to the appliance by two web applications: the Imprivata Admin Console and the Imprivata Appliance Console.

- **The Imprivata Admin Console** is used to configure the application (users, applications, policies, etc.) Access to the Imprivata Admin Console is controlled via application users imported from and integrated with Active Directory or created within the application directly.
  - There is delegated administration available in the Imprivata Admin Console to control administration rights and roles for application administrators.

    Imprivata strongly recommends an approach of least privilege, where administrators are limited only to functions or users that they need to manage.

    For example, a helpdesk team member may be able to manage a set of users, but not manage the configuration, applications, or audit records.
  - Token-based two factor authentication is directly available for the Imprivata Admin Console, and is recommended to be used.
  - The Imprivata Admin Console imposes a timeout period for inactive administrator sessions. In the Imprivata Admin Console, go to the **Settings** page, **System Settings** section to configure a timeout value of up to 90 minutes using the **Imprivata Admin Console Session Timeout**setting.
- **The Imprivata Appliance Console** is used to configure and manage the virtual appliances for enterprise configuration, bootstrapping, backups, restores, upgrades, SMTP, and NTP.

- The Imprivata Appliance Console ships with two pre-defined users: the Administrator and the Super-Administrator.

  Imprivata recommends using a very complex password and a Privileged Access Management system, for example, Imprivata Privileged Access Management, to manage these two appliance administrator credentials. For more information on Imprivata's Privileged Access Manager, see the Imprivata Privileged Access Management online help.
- Imprivata strongly recommends an approach of least privilege, where administrators are limited only to functions or users that they need to manage.
- Configure email notifications for consecutive login failures to the Imprivata Appliance Console and set automatic account disablement after a preset number of login failures. Configure these settings using the **Intrusion Detection Tab** of the **Security** page in the Imprivata Appliance Console.
- The Imprivata Appliance Console imposes a timeout period for inactive administrator sessions. In the Imprivata Appliance Console, go to the **System** page, **Settings** tab to set the auto logout time to up to 600 minutes (10 hours).

Audit Records Management

Keeping a good audit trail is essential to a strong records management strategy. It facilitates non-repudiation and the ability to have a definitive log on which administrator made what change at what time in the Imprivata Admin Console when a computer or use policy changes.

- Archive the results on a regular basis to a file share, so they are not solely on the Imprivata appliance.
- Use a secure method when archiving and storing audit records.
  - For transferring the audit records, use a secure method, such as secure SSH. The FTP protocol is not secure.
  - Store the audit records in a secure location.
- Balance the need for archived audit records carefully with performance considerations.

  You don't want to build up such a large set of audit logs that it adversely impacts the performance of the appliance. For this reason, Imprivata recommends that you use the **Archive and delete** option in Imprivata Admin Console.
- Archive the audit records for a period of two years, so you can use them for forensic investigations.

For more information, see "Managing and Maintaining Audit Records" in the Imprivata OneSign online help system.

Post to Syslog and Appliance Log Management

The Imprivata appliance has a system log. A portion of these logs can be transferred to a system log server. These event logs can be used for active alerting and in cases where forensics are needed when the Imprivata appliance is unavailable.

Set up a server to receive the system logs.

In the **Imprivata Appliance Console > System > Logs** tab, click **Edit** to configure a remote syslog server. Enter the IP address or hostname of the syslog server and enable TLS communication to secure it.

Configuring NTP

It is important to synchronize the enterprise's time to a single source of truth. It is critical when using Kerberos authentication or smart cards, as the local time of endpoints can drift over time. For forensics, it is important to have consistent timestamps in events.

Configure the NTP server in the Imprivata Appliance Console **> Network > NTP** tab. For more information, see "Managing NTP Server" settings in the Imprivata OneSign online help system.

Setting Up SMTP and Appliance Notifications

- Set up an SMTP server for the variety of appliance notifications sent to administrators.
- Set up email accounts that administrators will actively monitor.

Suspicious Email Alerts

Imprivata recommends that you configure email notifications of suspicious activity on the appliance or in Imprivata software applications, and login failures.

For more information, see *The Intrusion Detection Tab* in the Imprivata Enterprise Access Management online help system.

Reduce Login Failure

To reduce login failures, Imprivata recommends configuring several settings in the Imprivata Appliance Console.

For more information, see *The Intrusion Detection Tab* in the Imprivata Enterprise Access Management online help system.

Max bad attempts

Set this to a non-zero value.

Send Email Alert

Enable this setting.

Imprivata Admin Console Settings

Imprivata recommends the following Imprivata Admin Console settings.

Disable API Access

If you are not using API access for Imprivata Confirm ID, ProveID Web, or Imprivata ProveID Embedded, disable it.

On the API Access page in Imprivata Admin Console, select **Do not allow API access** from the drop-down lists.

Procedure Code Extensions

Procedure code extensions run any arbitrary script when a certain event occurs in the context of the user.

Security considerations should include:

- The area written to and what happens to the file.
- Whether the Administrator must perform a security review, because scripts can do damage.

For more information, see "Imprivata OneSign Extension Objects" in the Imprivata Enterprise Access Management online help system.

Imprivata Admin Console Session Timeout

The Imprivata Admin Console imposes a timeout period for inactive Administrator sessions. You can configure this value (up to 90 minutes) via the Imprivata Admin Console **Session Timeout** setting in the System Settings section of the Settings page.

SPML Provisioning

For SPML provisioning, enable the following settings:

- Enable IP access protection
- Enable Client Request Authentication

For more information, see "Using Imprivata Provisioning Features" in the Imprivata Enterprise Access Management online help system.

Directories

Use TLS for secure communication to Active Directory.

Appliance Backup

Consider the following items when configuring Imprivata appliances in your organization:

- For each appliance, schedule database backups for twice daily — one in the morning and one in the afternoon.

  The Imprivata database backup file contains the backup for the entire enterprise, not just a single site. The database backup does not back up the enterprise, agent, or appliance configuration files.
- Encrypt the backup file.
- Backups should use a secure file server, through the use of a SCP or network share.

Imprivata Agents

Consider the following items when configuring the Imprivata agent on endpoints in your enterprise:

- Use SSL Validation on all endpoints.
  - G4 appliances running 7.8 or later support TLS 1.3.

- G3 appliances running 7.4 or later support TLS 1.2.

  TLS 1.1 and TLS 1.0 are not supported.
- G3 appliances up to the 7.3 release support TLS 1.1 and TLS 1.2.

  TLS 1.0 is not supported.

The following Microsoft versions default to TLS 1.0:

- Windows Server 2008 R2
- Windows Server 2012

If your Windows endpoints are not already configured to use TLS 1.2 or higher, action may be required to prevent Imprivata agent to G3 appliance communication from failing on some agent versions.

If you are unsure of which endpoints are enabled for SSL validation, you can scan the Windows registry for the SSLValidation value of the **ISXAgent** registry key. The following table details this value:

Name	Location	Value
SSLValidation	32-bit: HKEY_LOCAL_MACHINE\SOFTWARE\SSOProvider\ISXAgent 64-bit: HKEY_LOCAL_MACHINE\SOFTWARE\SSOProvider\ISXAgent	Enabled=1 Disabled=0

Imprivata Enterprise Access Management Authentication Best Practices

Two Factor Authentication

Use two factor authentication for Imprivata Enterprise Access Management for SSO (formerly Imprivata OneSign) desktop authentication, Imprivata Enterprise Access Management for MFA (formerly Imprivata Confirm ID) remote access, and all signing workflows, especially EPCS.

The most common entry point for malware and ransomware attacks is via remote access with valid user credentials obtained via successful phishing.

Two factor authentication is available in a variety of combinations. For details, see "Configuring Authentication Methods in User Policies", "Imprivata Authentication Methods", and "Set Up Users" in the Imprivata Enterprise Access Management Help Portal.

Offline Authentication

Offline Authentication allows a user to log into Imprivata Enterprise Access Management even when the Imprivata agent cannot connect to the Imprivata server. The Imprivata agent uses cached encrypted credentials until it can contact the server again. In the Imprivata Admin Console, go to the **User policies** page > **Authentication** tab > **Desktop Access authentication**.

Security Questions

Users who forget or lose an ID token, smart card, or other authentication factor, can authenticate to Imprivata Enterprise Access Management by answering their security questions (emergency access).

Make security questions more secure: in the Imprivata Admin Console, select a user policy > **Authentication** tab > **Security questions**. Imprivata recommends:

- Require users to enroll 5 questions.
- Require users to answer 3 questions to authenticate.
- To prevent users from authenticating with security questions regularly, allow only 2 security question logins per month.
- Discourage the use of personal information as security answers when this personal information can be found on the Internet.

See "Authenticating to Imprivata via Security Questions (Q&A)" in the Imprivata Enterprise Access Management Help Portal.

User Challenges

Challenges help to maintain security after the Imprivata agent has been offline, especially in situations where more than one user has access to a computer. For higher security, Imprivata recommends:

- Require users to authenticate again when the Imprivata agent has returned online.
- Require users to authenticate again after the user has been inactive for 15 minutes.
- You can also require users to authenticate at a set time interval, even while the user has been active. However, this setting comes at a high cost in usability for the users, and is only recommended when the highest security is required.

In the Imprivata Admin Console, go to the **User policies** page > **Challenges** tab. For more information, see "User Challenges" in the Imprivata Enterprise Access Management Help Portal.

User Lockout

After a number of consecutive authentication failures, the user account is locked. Even if the user authenticates correctly during the lockout period, the account remains locked.

This setting applies to:

- Password Authentication
- Non-password authentication. For example, fingerprint or token
- Security questions (emergency access)
- Self-service password reset

In the Imprivata Admin Console, select a user policy and go to the **Lockout** section.

For complete details, see "User Lockout Policy" in the Imprivata Enterprise Access Management online help.

Best Practices — Passwords

Imprivata recommends following the password security standards as described by the National Institute of Standards and Technology (NIST). See the NIST Special Publication 800-63B for details.

- Require passwords greater than 12 characters in length.
- Set passwords to expire after 180 days. For every character over 12, you can extend the expiry date by 60 days. Changing passwords on a shorter interval is an unnecessary burden that does not increase security, and actually encourages users to compose weak passwords.
- Encourage the use of "pass phrases" that consist of a combination of words and special characters or numbers.

Best Practice — Default Passwords

Change default passwords for devices. Use robust passwords and make a record of them.

Locking Workstations

Computers in public or semi-public areas have the risk of being viewed by unauthorized people. Imprivata Enterprise Access Management provides a comprehensive set of tools for securing unattended workstations:

- Locking workstations with a hotkey and badge tap
- Secure Walk Away — automatic walk–away security based on the proximity of your users' mobile phones
- User Notifications at unattended workstations — to display the name of who's currently logged into a shared workstation.
- Inactivity-based presence detection — the workstation locks when Imprivata Enterprise Access Management fails to detect activity after a specified period of time.

Use Secure Walk Away in conjunction with Inactivity Detection set to 15 minutes or less, in an environment where users share workstations and need to leave workstations in a hurry (ED or Wards, for example). See "Configuring Walk-Away Security for Unattended Workstations" in the Imprivata Enterprise Access Management online help.

Computer Policies Overriding User Policies

User policies take precedence over computer policies, but when you need to apply especially strict security to specific computers, Imprivata recommends **Override and Restrict** settings. Use Override and Restrict settings to enforce stricter security policies for a specific group of computers. See "Setting Computer Policies to Override User Policies" in the Imprivata Enterprise Access Management online help.

Imprivata Enterprise Access Management Single Sign On

In addition to improving user experience, Imprivata Enterprise Access Management Single Sign On is a tremendous security benefit to your enterprise. The fewer passwords your users use, and the less often they manually enter passwords, the more secure your enterprise can be.

When you deploy an Imprivata application profile to users, you should pay careful attention to security settings.

- Allowing users access to Imprivata Single Sign On when the Imprivata agent is offline
- You can enable users to edit their Imprivata SSO application credentials
- You can enable users to reveal their passwords in the Imprivata password manager or in the Password Self Services feature
- You can prohibit users from bypassing Imprivata SSO for specific applications
- You can program a finite lifespan for single sign-on data used by offline-enabled users. This provides a guaranteed limit to how long an offline-enabled user can access the network if the user’s account was closed while the user was offline.

For complete details, see "Single Sign-On Security Settings" in the Imprivata Enterprise Access Management online help.

Remote Access — Temporary Codes

When Imprivata ID authentication is required to log in, but the user doesn't have his device or OTP token, Imprivata has made it easy for your enterprise to issue a temporary code allowing your user to continue their work virtually uninterrupted. Temporary codes can also be used when you need to provide remote access to a temporary user such as a contractor.

It's important for your helpdesk to implement security protocols around issuing temporary codes. Validating the identity of a person who is requesting a temporary code for an Imprivata account is essential to maintaining the security of that account.

See "Temporary Codes for Remote Access" in the Imprivata Enterprise Access Management online help.

Remote Access — Skip Second Factor

You can allow users associated with the MFA Remote Access workflow to skip the second authentication factor. Select how long the user can skip second factor (1 hour minimum — 120 days maximum). The default is 30 days.

To improve the security of your enterprise, do not allow users to skip the second authentication factor. See "Skip Second Factor" for Remote Access in the Imprivata Enterprise Access Management Help Portal.

Revoke EPCS from a User

The **Delete Record** function can be used to revoke the ability to e-prescribe controlled substances from a user. See "Delete Record and Revoke EPCS" in the Imprivata Enterprise Access Management Help Portal.