Using IAM and PAM

to Enable and Secure Remote Work
During the COVID-19 Lockdown
Contents

1 Introduction 1

2 Pre-existing versus new telecommuters 2

3 Surging capacity 3

4 Accessing on-premises versus cloud-delivered applications 4

5 IT workers 5

6 Passwords and other credentials 6
   6.1 Secure logins to Internet-accessible services 6
   6.2 Notify users of password expiry 6
   6.3 Resolve problems with locally cached passwords 6

7 Planning for a return to normal 8
   7.1 Forgotten and expired passwords on return 8
   7.2 Reactivating access 8
   7.3 Adjusting access rights 8

8 How Hitachi ID Systems can help 10
1 Introduction

The COVID-19 pandemic has led governments around the world to require citizens to stay at home for an undetermined duration, likely several months. This is incredibly disruptive to economic activity. Where possible, employers have asked their workers to continue to work, but remotely.

In this document we consider the impact on IT infrastructure of abruptly transitioning large portions of an organization's workforce to telecommuting status and how identity and access management (IAM) and privileged access management (PAM) systems can help with some of the challenges created by this transition.
2 Pre-existing versus new telecommuters

The pandemic-driven transition from workers coming into offices to the same workers connecting from home was abrupt in most jurisdictions. This means that organizations did not have time to go through their usual process to provision people who normally work at the office with laptops, VPN credentials, strong authentication apps or hardware, instructions, etc.

This means that in most organizations there are now two profiles of telecommuters:

1. Legacy telecommuters, typically using a corporate-provisioned, centrally-managed laptop, VPN software and MFA authentication.

2. New telecommuters, typically using a home PC or personal laptop, possibly without access to the corporate VPN and possibly logging in with a single factor (a password).

For the legacy telecommuters, the technology required to telecommute is a continuation of business as usual. The only difference is that they are now permanently telecommuting, which means that some processes may break down. Specifically, there may be password-related problems:

1. If the user doesn't connect to the VPN, they may not be warned of password expiry.

2. If the user changes and subsequently forgets their locally cached AD password, they may not be able to resolve the login problem, because while the help desk can reset an AD password on the network, the help desk cannot reach into an off-line PC to replace the locally cached copy of that forgotten password.

New telecommuters can access SaaS applications from their home PC without issue, but may present a variety of challenges:

1. Access requests may have to be processed to grant new telecommuters access to remote work services, such as VDI logins or MFA applications.

2. It may be necessary to (rapidly) migrate some services to the cloud, such as moving mailboxes from on-premises Exchange to Office 365. This is so that users without corporate laptops or VPN connections can continue to function using nothing more than a web browser and Internet connection.

3. These users may have to access on-premises applications using a VDI infrastructure placed at the organization's network perimeter – i.e., users can establish VDI sessions from the Extranet and the VDI sessions can access services on the private corporate network.

4. Since SaaS and VDI login screens are typically accessible at a public URL, strong authentication is strongly advised, to prevent compromise of user logins on critical applications by external attackers who guess or socially engineer user passwords.
# 3 Surging capacity

The abrupt transition to working from home means that an organization’s facilities to support telecommuting may have to grow abruptly. This may include:

1. Voice-over-IP telephony, so that users can continue to make phone calls over corporate infrastructure, for example avoiding long distance charges on their mobile or home phone.
2. Support for videoconferencing, typically via third party providers such as Microsoft, Google, WebEx or Zoom, to replace in-person interactions.
3. Expanded data bandwidth, especially for VPN access to the corporate network.
4. Expanded virtual private network licenses (for more users) and/or bandwidth and/or CPU capacity, to handle more concurrent connections by more users.
5. Expanded virtual desktop infrastructure (VDI) server farms, to support remote work by users who previously worked on-site.
6. Procurement of new managed laptops for telecommuters who cannot be fully productive using their home PCs (or who don’t have one).
7. Licensing multi-factor authentication technology, preferably via smart phone apps, to reduce the risk due to password-only logins to services reachable at a public URL.
4 Accessing on-premises versus cloud-delivered applications

Users with either a corporate laptop or home PC can access the Internet, which means that they can sign into SaaS applications such as Office 365, Google Apps, WebEx, etc. This is the simplest model for telecommuting and the lockdown will undoubtedly accelerate the transition in many organizations from on-premises software to software as a service.

When applications are deployed on-premises, telecommuters have three options:

1. Defer access until on-premises access is possible again.
2. Sign into a VDI session and access applications from there.
3. Establish a VPN connection from either a corporate or personal endpoint device and connect to the on-premises application over this connection.

Each of these (even the first!) has its own pros and cons:

1. The do-nothing option is obviously simplest and least costly from an IT service perspective, but presumably also the most disruptive to the business. This is a surprisingly popular option, especially where the users in question are blocked from work in general, due to inability to access their usual workplace. For example, consider workers in a courtroom, where cases are deferred due to the lockdown.

2. The VDI option reduces the risk due to compromised user devices being attached to the corporate network but likely requires increased VDI server capacity, additional VDI software licenses and is inconvenient for users who must first sign into their desktop or laptop, then into the VDI session and finally into the desired application.

3. The VPN option is typically more complex for users to configure, especially without personal hand-holding from IT to get started. If users connect from a personal device, this approach also expands the corporate network perimeter to include unmanaged and possibly insecure or compromised devices. However, it does not require as much physical infrastructure as the VDI approach, may incur lower incremental software license fees as compared to VDI and may reduce the number of screens that users have to sign into before they reach desired applications.
5 IT workers

IT workers are likely to face an increased workload as they assist their organizations in transitioning to 100% telecommuting, or as close to that as possible. These workers need to access a wide variety of systems and applications, many of which are still on-premises in most organizations. IT workers are also likely to already be able to work remotely, so VPN access is not a big problem.

Some IT work must be done on-site, as it requires physical contact with hardware. This includes racking new servers (due to increasing demand!) and resolving physical problems with hardware or networks.

IT work typically involves elevated access to facilities, systems and applications. To secure this, multi-factor authentication, robust authorization models and detailed forensic audits are required. Static passwords are to be avoided and shared passwords must be periodically changed, encrypted, vaulted and injected into login sessions rather than displayed. These capabilities should sound familiar – they are the basic features of a modern privileged access management (PAM) system.

In the context of a lockdown, vendor access is even more likely to be remote than before. To secure vendor access, systems are required to:

1. Delegate the management of users within each vendor organization to a trusted individual at that organization. For example, if an organization sources servers from Dell, storage arrays from Hitachi Vantara and database software from Oracle and Microsoft, then they should designate one person at each of those firms to manage the small list of other people at their own firm who can sign into the organization's systems to provide support.

2. Ensure that logins by vendor staff are securely authenticated, using multiple factors (not just passwords). Since vendor users may turn over with some frequency, it's much easier (and cheaper!) to use app-based MFA than physical tokens for this.

3. Optionally, ensure that a given user is still employed by the authorized vendor whenever they sign in. This can be done by sending a PIN to the user's work e-mail at login time. If they have left the vendor organization, they won't be able to retrieve the PIN and so won't be able to sign in.

4. Use a request/approval workflow prior to allowing vendor users to sign into systems. Vendor users should connect when asked to perform work, not at will.

5. Record and optionally watch in real time vendor activity.

6. Inject randomized, vaulted passwords into vendor login sessions.

7. If possible, do not connect vendor endpoint devices to the corporate VPN. This eliminates the need to review the security posture of every such device. Instead, connect vendor sessions through a proxy – such as a VDI system or by rendering login sessions in a browser tab. This keeps the vendor user's device outside of the corporate network perimeter and so reduces the organization's attack surface.

None of these capabilities should be novel or surprising – they are best practices for granting elevated access to third party users, using a PAM system.
6 Passwords and other credentials

Whether working on-site or remotely, users authenticate into login sessions to perform work. Even in organizations that adopt “passwordless” authentication – logins still happen, but instead of knowledge factors, some combination of hardware, biometrics and cryptographic keys are used.

6.1 Secure logins to Internet-accessible services

The first and most important consideration for telecommuting is that some services are reachable at public Internet addresses, via public URLs. This may include SaaS application logins and VDI session logins. Public URLs can be attacked by anyone with an Internet connection. In 2019, there were about 4 billion Internet users – that is the population of potential attackers. Given the large population of possible attackers, it is important to protect these services. Multiple authentication factors are a good starting point:

1. Externalize login screens from all services that expose a public URL via federation, typically using SAML.
2. Implement multi-factor authentication on the federated identity provider.
3. The “knowledge factor” – a password, PIN or answers to security questions – should be presented to the user last, because this factor may be vulnerable to guessing. It is better for users to first interact with a hardware token, enter a PIN sent to their phone or use a smart phone app and only then, if they have successfully completed this login step, should they be prompted for their password or other secret.
4. Consider a CAPTCHA as the first authentication step, to ensure that the entity signing in is indeed a human, and not a scripted 'bot carrying out an algorithmic attack on the login page.

6.2 Notify users of password expiry

Most employees and contractors will continue to have login IDs and passwords on on-premises systems and applications, including on the corporate Active Directory domain. Windows only warns users of impending password expiry when they sign into a domain-joined PC with a network connection, either on-site or through a VPN. The absence of a warning about password expiry does not imply that passwords will not expire – it just means that users will be surprised when their passwords have expired. It is therefore important to implement an alternate mechanism to warn users of upcoming password expiry, for example via e-mail, and to enable them to change their soon-to-expire passwords while away from the office.

Alternately, consider temporarily extending the password expiry time window, for the duration of the lockdown.

6.3 Resolve problems with locally cached passwords

Legacy telecommuting users typically have a corporate laptop and sign into that device with a locally cached copy of their Active Directory password. They also typically establish a VPN connection and so will be
periodically prompted to change their AD password. New passwords set locally (i.e., via the Ctrl-Alt-Delete user interface) will be stored both locally and on AD domain controllers.

If a telecommuting user changes their AD password and subsequently forgets it, then they have a serious problem:

1. They can call the help desk and arrange for their AD password to be reset.
2. The new AD password has no way to propagate back to their device.
3. The help desk has no way to update the password cached locally on their device.

Since the forgotten password is needed to unlock the device, the device becomes inoperable.

Under normal circumstances, such a user could bring their laptop into the office. A login attempt there, when the laptop is wired into the corporate network, will succeed because an AD DC with the new password is accessible. The new password will then be cached locally.

Without the ability to visit the office, this problem becomes much more severe, necessitating a remote mechanism to resolve forgotten, locally cached passwords. Hitachi ID Password Manager (perhaps uniquely among password reset software products) includes a mechanism for this purpose.
Planning for a return to normal

Forgotten and expired passwords on return

Some users will have stopped login activity during the lockdown. This may be because their work was suspended (layoff, etc.) or because access to some systems or applications was not required during the lockdown. In either case, when these users return to work, they will need to sign on again and may experience problems:

1. It has been months since their last login, and they have forgotten their password.
2. Their password has expired in the intervening time.

It is important to estimate the number of users who have not signed on for an extended period of time, because a large proportion of these will require login assistance simultaneously and this could easily be a high-delay, high-stress day for the IT support organization.

It is also advisable to plan for and communicate a strategy for these people to reset forgotten passwords when they get back to business as usual. For example, on a one-time-only basis, these users might click on a link with an embedded random PIN to sign into the password reset system and select a new password that way. This eliminates problems both with forgotten answers to security questions and forgotten passwords.

Reactivating access

In organizations where a significant number of people were furloughed, a plan is required to reactivate access when workers return. If everyone will return at the same time, then an automated process that operates on a list of identities is more appropriate. On the other hand, if people return to work more gradually, then a request/approval workflow will work best. In either case, an IAM system is the right tool for the job.

Adjusting access rights

When people return to to work, their roles and responsibilities may be a bit different than prior to the pandemic, due to the changing economic reality. To accommodate this, it is appropriate to review everyone’s access rights. In particular, the assigned job role may have to be adjusted and previously assigned entitlements may no longer be appropriate.

This kind of review is exactly access certification:

1. A review of role is a certification of a key profile attribute (role ID).
2. A review of existing entitlements is a certification of assigned technical roles, accounts and group memberships.
Using IAM and PAM to Enable and Secure Remote Work

Given the large number of people whose identity attribute(s) and entitlements will be reviewed, the most scalable model is to invite each user’s manager to review that user’s data. This is an org-centric access certification campaign.

As with post-furlough reactivation above, this is classical IAM functionality.
8 How Hitachi ID Systems can help

As described throughout this document, the lockdown presents organizations with many challenges, some of which can be addressed with IAM and PAM solutions. Following are the various ways in which Hitachi ID Systems software can help:

1. **Granting and revoking access:**
   As users switch to working remotely, *Hitachi ID Identity Manager* can be used to ensure they are provisioned access to VPN or VDI platforms. This is typically done by creating accounts or assigning group memberships. Requests for these changes may be submitted via automation (e.g., for all users matching some criteria) or via the *Identity Manager* request portal.

2. **Terminations and furloughs:**
   If organizations are forced to downsize, requests to deactivate access permanently or to place staff on a leave of absence can likewise be processed by *Identity Manager*. Temporary leave is implemented by deactivating login IDs and setting a status on each user profile. Permanent deactivation is modeled in the same way, but with additional steps to move and archive content on home directories, mail systems, etc.
   In either case, requests to place people on leave or deactivate their access can be submitted either via automation (based on authoritative data and inclusion criteria) or via a request/approval workflow.
   In the case of furloughs, when workers return, the same mechanisms can be used to reactivate access.

3. **Password expiry notification:**
   When workers transition to telecommuting, they may no longer be prompted to change their passwords, and expiration will be abrupt and disruptive. *Hitachi ID Password Manager* can be used to identify users with soon-to-expire passwords, to notify them of this and to facilitate password changes.

4. **Forgotten, locally cached passwords:**
   Users who forget their passwords and who use a corporate laptop, where that password is cached locally, cannot easily resolve their login problem. *Password Manager* includes a mechanism called "Self-Service, Anywhere" that integrates with the PC login screen, WiFi stack and corporate VPN and enables users who are locked out of their PC, even when off-site, to both reset a forgotten password and (most importantly!) to update the locally cached password to the new value. This allows users to resolve a very disruptive login problem without having to come into the office.

5. **Strong, multi-factor authentication:**
   As users move to working remotely, they access systems (such as VDI infrastructure) and applications (such as SaaS) that expose a login screen at a public URL. These login screens need to be secured more carefully than application logins on the private corporate network, because the set of possible attackers is very large.
   *Password Manager* includes a SAML 2.0 federated access identity provider, an application launchpad and multi-factor authentication, using a smart phone app. All of these can be leveraged to ensure that logins to all systems and applications reachable from the public Internet require multiple authentication factors.

6. **Secure, remote access to administrative logins:**
   IT staff are required to transition to remote work just like everyone else. The difference is that IT staff sign into high-privilege accounts like `root` on Unix/Linux and `Administrator` on Windows/AD.
These logins typically do not support multi-factor authentication, and shared accounts normally have static, well known passwords. To eliminate these security vulnerabilities, a PAM system such as Hitachi ID Privileged Access Manager is required. This randomizes and vaults passwords, strongly authenticates and personally authorizes access, brokers logins (single sign-on for admins) and may even be configured record activity to create a forensic-quality audit trail.

Note that Privileged Access Manager includes Hitachi ID Mobile Access, which enables multi-factor authentication (MFA) in case an organization has not already provisioned an MFA system for all IT workers.

PAM controls are even more important when people work remotely, as they may connect from personal devices. These connections extend the physical network perimeter and originate from devices whose security may not be assured.

7. **Secure, remote access for vendors:**

   Identity Manager and Password Manager can be used to delegate the management of vendor identities and credentials out to each vendor. Password Manager also enables all vendor users to leverage Mobile Access for strong, multi-factor authentication.

   Combining this with Privileged Access Manager, vendor users can launch login sessions subject to a request/approval workflow and session monitoring (both real-time and recorded/searchable). SSH and RDP sessions, in particular, can be established from a web browser, eliminating the need for either a VPN connection or any particular client software configuration on vendor users PCs.