

## Introduction

Ironsphere provides privileged access security capabilities based on a man-in-the-middle architecture to prevent credential theft of super-user accounts, and ensures they are used only for legitimate business purposes. Direct Access refers to the accidental or intentional access attempts from users' computers to remote hosts/servers directly, instead of through Ironsphere. sPrivileged user direct access management can be approached in 4 different ways:

1. Changing the owner of the privileged credentials (from users to Ironsphere)
2. Blocking direct access at the network level

3. Detecting and responding to direct access attempts
4. Deploying Access Control Agent on Hosts/Servers

These options can be used individually or combined in a single deployment. This decision will be primarily driven by the nature of the infrastructure and the desired level of control/security. For details on each approach, please refer to the Ironsphere "Direct Access Management" Solution Brief.

This solution brief details the 4th option – Deploying Access Control Agent on Hosts/Servers – specifically as it applies to Windows Servers.

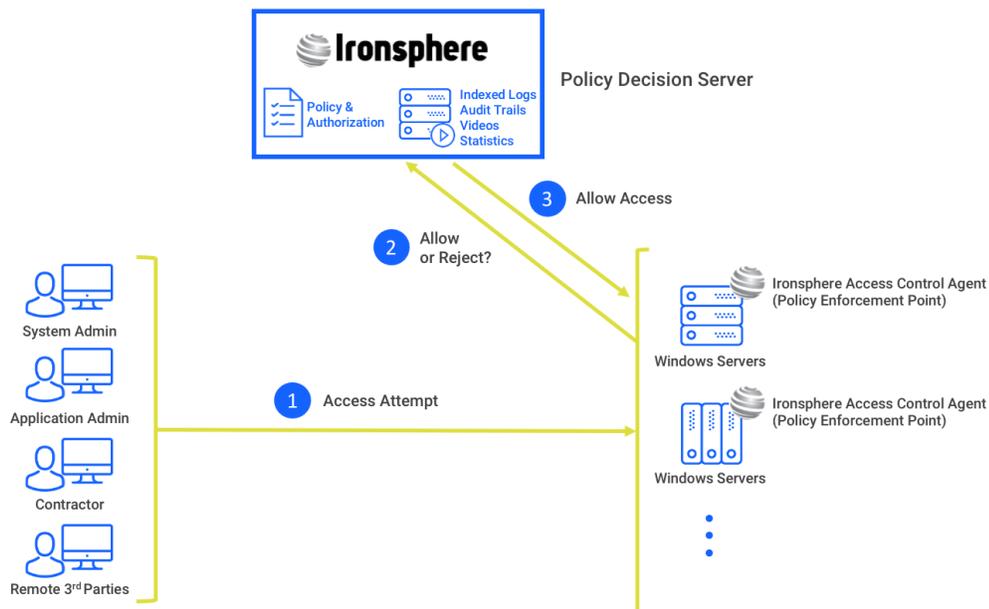


Figure 1—Deploying Access Control Agent on Windows Servers

The Access Control Agents run on target hosts/servers (in this case Windows servers) and detect user remote desktop access attempts, regardless of the source or type of attempt. Once the Access Control Agent detects a remote desktop access attempt on a windows server, it manages whether or not the user is allowed to connect, and limits the applications that user will be allowed to run, via a centralized server. The access permission and

application isolation policies are managed by the central Ironsphere server (i.e., Policy Decision Server) and enforced by the Ironsphere Access Control Agent (i.e., Policy Enforcement Point) on Windows servers. All access attempts, session details, and user activity are tracked by the Access Control Agent and sent to the central server, enabling unified visibility into user activity throughout all windows servers in the organization's technology infrastructure.

## Direct Access Management

The Access Control Agents running on Windows servers handle user remote access attempts, allowing or denying access through a centralized server. If the user is part of the central server allowlist, the submitted credentials are forwarded to the Active Directory server to complete

authentication. The Ironsphere server, in combination with the Access Control Agents, enables organizations to implement segregation of duties practices, by eliminating unsupervised user access, and centrally managing which users can access which servers.

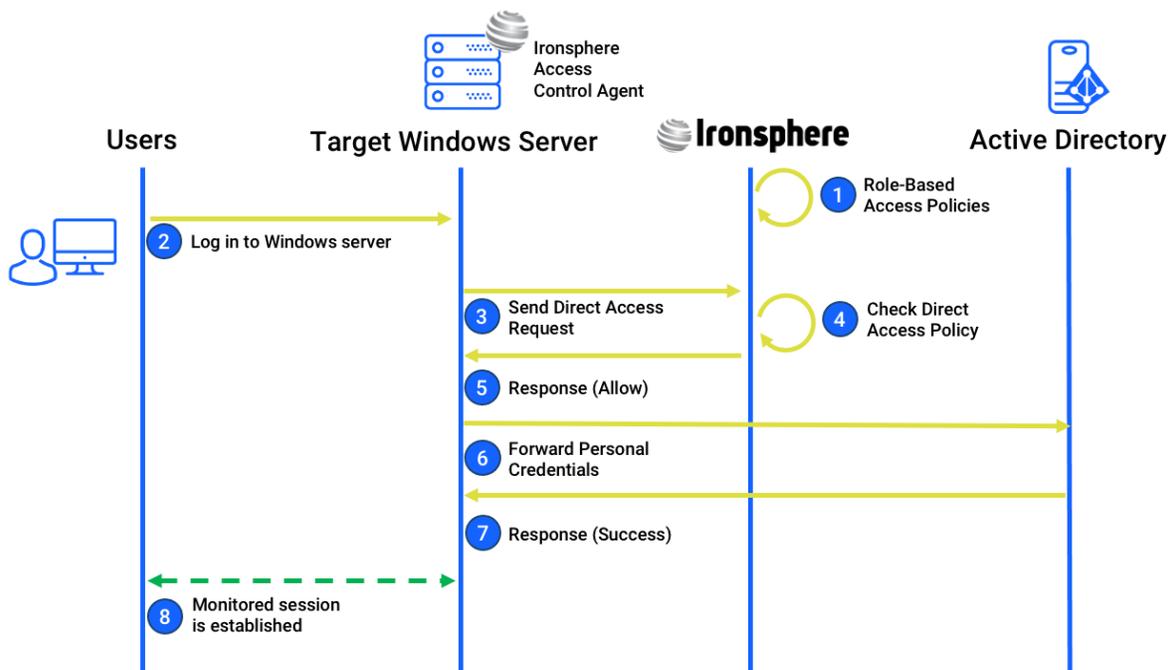


Figure 2 – Direct Access Management Flow

**Role-based Access Policies:** Access policies regarding which users have direct access permissions to which windows servers should be configured properly in the Ironsphere server as a one-off initial setup

**Log In to Windows server:** User attempts to log in to the remote Windows server from an RDP client application running on his/her computer, using personal credentials (e.g., personal account on Active Directory)

**Send Direct Access Request:** Access Control Agent forwards user access attempt to centralized Policy Decision Server, i.e., Ironsphere server

**Check Direct Access Policy:** Ironsphere server checks whether or not the user is allowed to access the target Windows server directly

**Response (Allow):** Ironsphere server sends response ("allow" in this case) to the Ironsphere Access Control Agent

**Forward Personal Credentials:** Once the Access Control Agent receives the "allow" response from the Ironsphere server, it sends the user's personal credentials to the Active Directory server

**Response (Success):** If the user's personal credentials are correct, the Active Directory sends a success response to the Access Control Agent

**Monitored Session is Established:** A monitored session between the user's computer and the remote windows server is successfully established

## In-Session Privilege Management

Once the session between the user's computer and the Windows server is established, the Access Control Agent running on the server tracks all user activity and handles the user's privilege elevation requests. The Ironsphere Access Control Agent detects any user attempts to run an application on the Windows server at the operating system level, and forwards the request to the centralized Policy Decision Server, i.e., Ironsphere server. Depending

on the response received from the Ironsphere server, the Access Control Agent either allows or blocks the user from running the application. Ironsphere's In-Session Privilege Management capability enables organizations to implement least privilege management practices by providing central management of what users can and cannot do on servers, based on their roles in the organization.

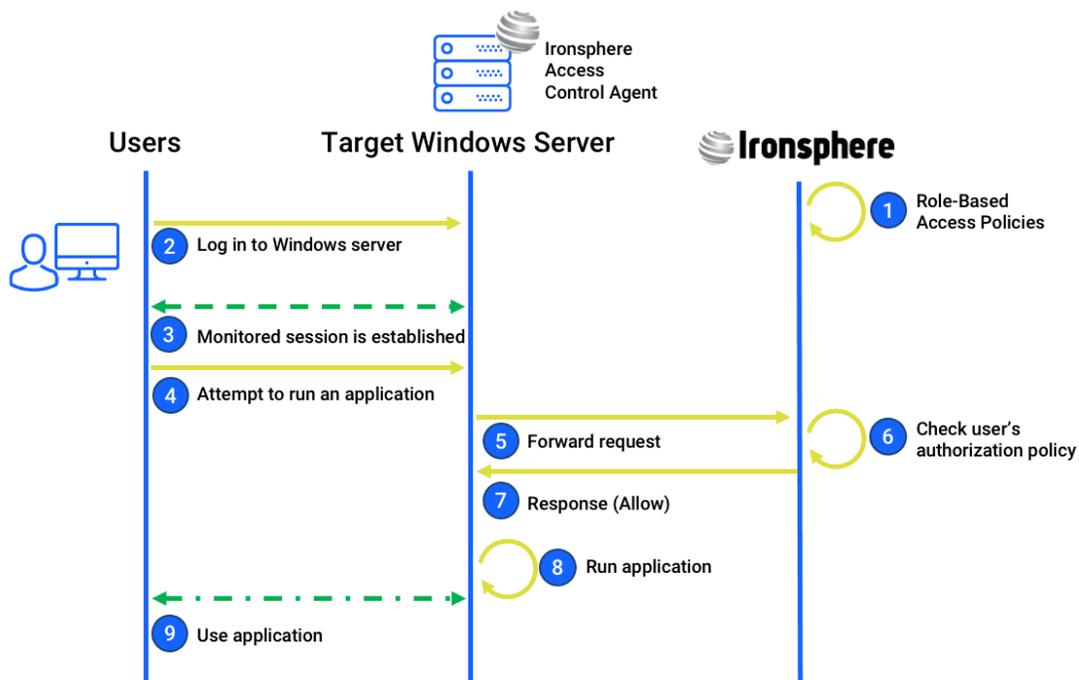


Figure 3 – In-Session Privilege Management Flow

**Role-Based Access Policies:** Access policies regarding which users are allowed to run which application on which windows servers, should be configured properly as a one-off initial setup

**Log In to Windows Server:** User attempts to log in to the remote Windows server from an RDP client application running on his/her computer, using personal credentials (e.g., personal account on Active Directory)

**Monitored Session is Established:** A monitored session between the user's computer and the Windows server is successfully established

**Attempt to Run an Application:** User attempts to run an application on the target Windows server

**Forward Request:** Ironsphere Access Control Agent detects the user's attempt to run an application at operating system level and forwards this request to the Ironsphere server

**Response (Allow):** Ironsphere server sends response ("allow" in this case) to the Ironsphere Access Control Agent

**Run Application:** Ironsphere Access Control Agent starts the application

**Use Application:** Application is started on the Windows server and is ready for remotely use

## Unified Visibility and Audit Trails

The Ironsphere Access Control Agent tracks, monitors, and logs all user activity on the Windows server, and sends all logs to the Ironsphere server at regular intervals. Audit trails from all Access Control Agents are collected by the Ironsphere server, providing

unified visibility to assist with security operations, internal audits, and regulatory compliance. All log records are indisputable, and available in human-readable, searchable indexed format, to help with incident management and forensic activities.

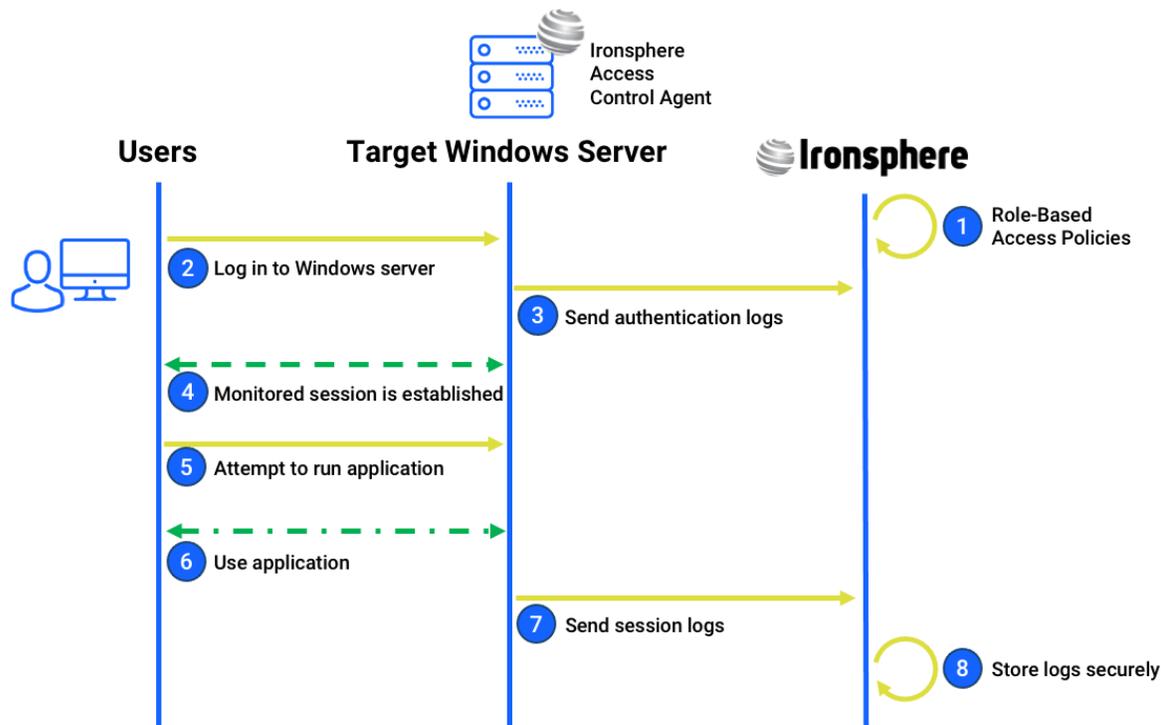


Figure 4 – Log Management Flow

**Role-based Access Policies:** Access policies regarding which users have direct access to which windows server, and are allowed to run which applications, should be configured properly as a one-off initial setup

**Log In to Windows Server:** User attempts to log in to the remote Windows server from an RDP client application running on his/her computer, using personal credentials (e.g., personal account on Active Directory)

**Send Authentication Logs:** User Authentication attempt (whether successful or not) is logged by the Ironsphere Access Control Agent, and those logs are forwarded to the central Ironsphere server at regular intervals

**Monitored Session is Established:** After a successful authentication, a monitored session between the user's computer and the Windows server is successfully established

**Attempt to Run an Application:** User attempts to run an application on the remote Windows server

**Use Application:** Application is started on the Windows server and is ready for remote use

**Send Session Logs:** Ironsphere Access Control Agent logs all user activities and applications executed in the session, and sends those user activity log records to the central Ironsphere server at regular intervals

**Store Logs Securely:** Ironsphere server collects log records from the Access Control Agent and securely stores them to be used in reports and forensic activities

## Conclusion

Ironsphere is the fastest to deploy PAM solution in the market due to its agentless man-in-the-middle architecture. The recommended approach is to isolate all privileged sessions and establish them through Ironsphere, eliminating user direct access to remote hosts/servers. If an organization has special edge cases or exceptional use cases, where direct access of privileged users cannot be monitored or eliminated, Ironsphere Access Control Agents can be deployed as a complementary capability to centrally manage privileged user direct access.

Access Control Agent based deployment provides the following direct access capabilities to manage such exceptional or edge use cases:

- Segregation of duties: central management of which users have direct access to which servers
- Single-Sign-On: enable users to log in to Windows servers with their personal accounts on Active Directory
- Multi-Factor Authentication: additional security layer to ensure the person accessing Windows server is who they claim to be
- In-Session Least Privilege Management: central management of which users can or cannot run which applications on remote Windows servers
- Role-Based Privilege Management
- Unified Visibility and Audit Trails of all user activities during direct access sessions

