Solution Brief

# Direct Access Management for Network Elements

Ironsphere
A Krontech Company

## 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. Privileged 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 Agents 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 Agents on Hosts/Servers – specifically as it applies to network elements.

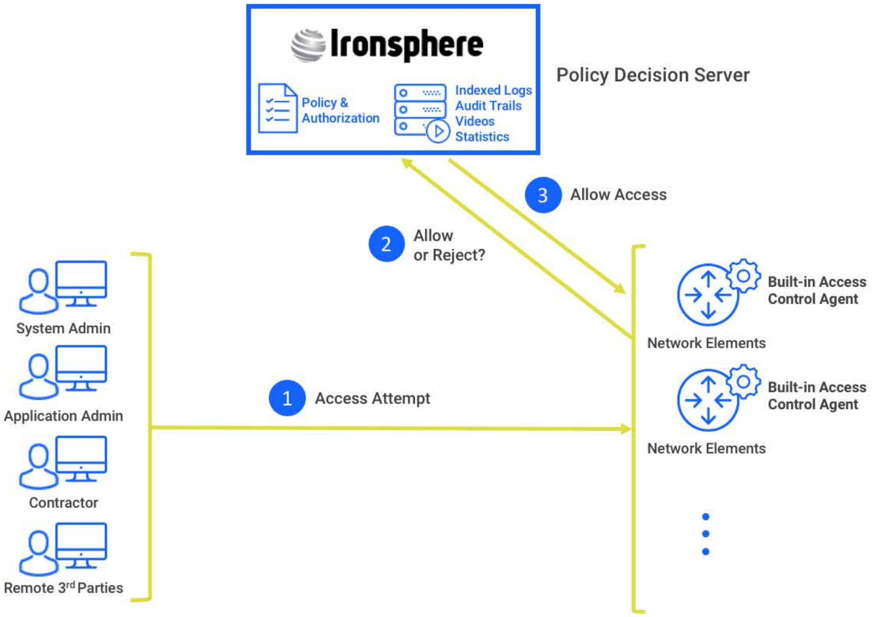

*Figure 1—Deploying Access Control Agent on Network Elements*

The built-in Access Control Agents run on target network elements and detect user remote console access attempts, regardless of the source or type of attempt. Once the Access Control Agent detects a remote console access attempt on a network element, it manages whether or not the user is allowed to connect, and limits the commands that user will be allowed to execute, 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 built-in Access Control Agent (i.e., Policy Enforcement Point) on the network element. All access attempts, session details, and user activity are tracked by the built-in Access Control Agent and sent to the central server, enabling unified visibility into user activity throughout all network elements in the organization's technology infrastructure.

## Direct Access Management

The built-in Access Control Agent running on network elements handles 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 Ironsphere server to complete authentication.

The Ironsphere server's built-in TACACS and RADIUS Servers, in combination with the built-in Access Control Agent, enable organizations to implement segregation of duties practices, by eliminating unsupervised user access, and centrally managing which users can access which servers.

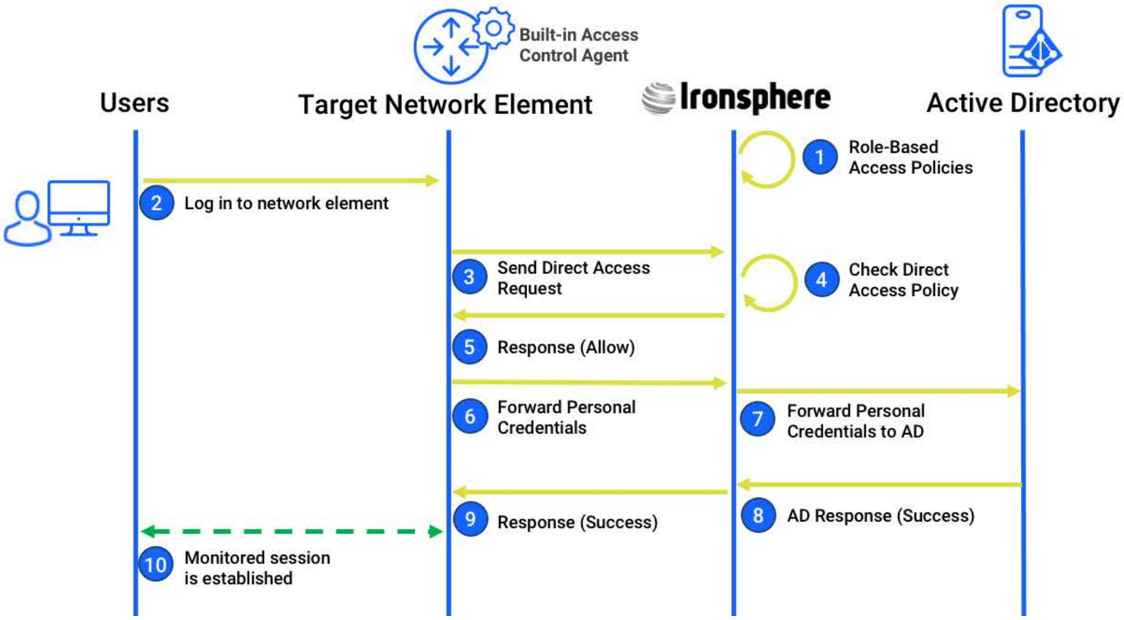
Built-in Access Control Agent
Users
Target Network Element
Ironsphere
Active Directory
1 Role-Based Access Policies
2 Log in to network element
3 Send Direct Access Request
4 Check Direct Access Policy
5 Response (Allow)
6 Forward Personal Credentials
7 Forward Personal Credentials to AD
8 AD Response (Success)
9 Response (Success)
10 Monitored session is established

*Figure 2 — Direct Access Management Flow*

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

**Log In to Network Element:** User attempts to log in to the remote network element from an SSH/Telnet 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 network element directly

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

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

**Forward Personal Credentials to AD:** If the personal account is a local account on the Ironsphere server, the Ironsphere server validates the credentials internally. If the personal account is a remote account on Active Directory, as depicted in the diagram above, Ironsphere forwards the credentials to the Active Directory server

**AD Response (Success):** If the user's personal credentials are correct, the Active Directory server sends a success response to the Ironsphere server

**Response (Success):** Ironsphere server sends a success response to the built-in Access Control Agent

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

## In-Session Privilege Management – TACACS

Once the session between the user's computer and the network element is established, the built-in Access Control Agent running on the server tracks all user activity and handles the user's privilege elevation requests. The built-in Access Control Agent detects any user attempts to execute a command on the network element 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 built-in Access Control Agent either allows or blocks the user from executing the command. 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 network elements, based on their roles in the organization.

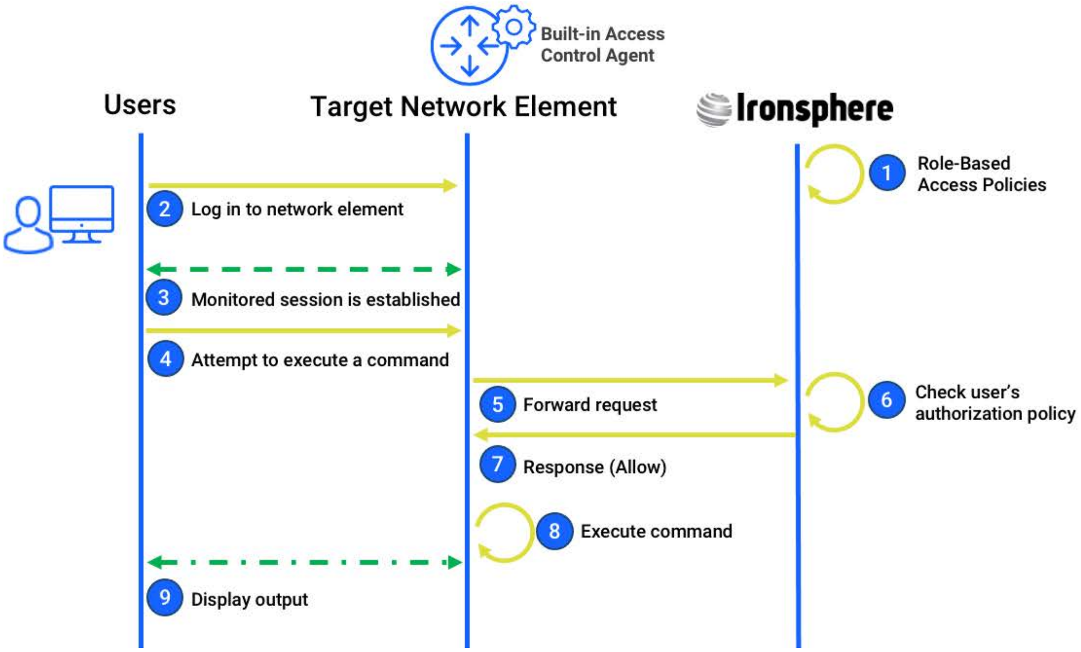
Built-in Access Control Agent
Users
Target Network Element
Ironsphere
1 Role-Based Access Policies
2 Log in to network element
3 Monitored session is established
4 Attempt to execute a command
5 Forward request
6 Check user's authorization policy
7 Response (Allow)
8 Execute command
9 Display output

*Figure 3 — In-Session Privilege Management Flow–TACACS*

**Role-Based Access Policies:** Access policies regarding which users are allowed to execute which commands on which network element, should be configured properly as a one-off initial setup

**Log In to Network Element:** User attempts to log in to the remote network element from an SSH/Telnet 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 network element is successfully established

**Attempt to Execute a Command:** User attempts to execute a command on the remote network element

**Forward Request:** The built-in Access Control Agent detects the user's attempt to execute a command at the operating system level, and forwards this request to the Ironsphere server

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

**Execute Command:** The built-in Access Control Agent executes the command

**Display Output:** Command is executed on the network element and output is displayed

## In-Session Privilege Management – RADIUS

Once the session between the user's computer and the network element is established, the built-in Access Control Agent running on the server tracks all user activity and handles the user's privilege elevation requests. The built-in Access Control Agent request user privileges from the centralized Policy Decision Server, i.e., Ironsphere server at the beginning of the session. Depending on the response received from the Ironsphere server, the built-in Access Control Agent either allows or blocks the user from executing the command. 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 network elements, based on their roles in the organization.

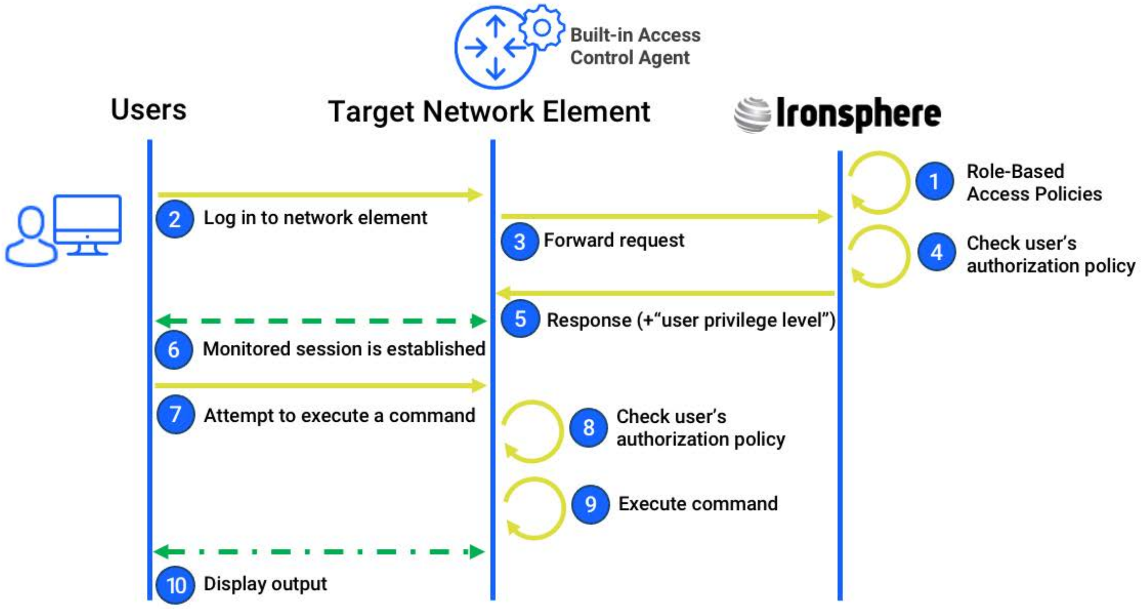
Built-in Access Control Agent
Users
Target Network Element
Ironsphere
1 Role-Based Access Policies
2 Log in to network element
3 Forward request
4 Check user's authorization policy
5 Response (+"user privilege level")
6 Monitored session is established
7 Attempt to execute a command
8 Check user's authorization policy
9 Execute command
10 Display output

*Figure 4 — In-Session Privilege Management Flow–RADIUS*

**Role-Based Access Policies:** Access policies regarding which users are allowed to execute which commands on which network element, should be configured properly as a one-off initial setup

**Log In to Network Element:** User attempts to log in to the remote network element from an SSH/Telnet client application running on his/her computer, using personal credentials (e.g., personal account on Active Directory)

**Forward Request:** The built-in Access Control Agent forwards the request to the Ironsphere server

**Check User Authorization Policy:** Ironsphere server checks user authorization policy

**Response (+ "user privilege level"):** Ironsphere server sends user privilege level to the built-in Access Control Agent

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

**Attempt to Execute a Command:** User attempts to execute a command on the remote network element

**Check User's Authorization Policy:** The built-in Access Control Agent executes the command if the privileged level of the user is sufficient to execute the command according to the user attributes

**Execute Command:** The built-in Access Control Agent executes the command

**Display Output:** Output of command execution is displayed

## Unified Visibility and Audit Trails

The built-in Access Control Agent tracks, monitors, and logs all user activity on the network element, and sends all logs to the Ironsphere server at regular intervals. Audit trails from all the built-in 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.

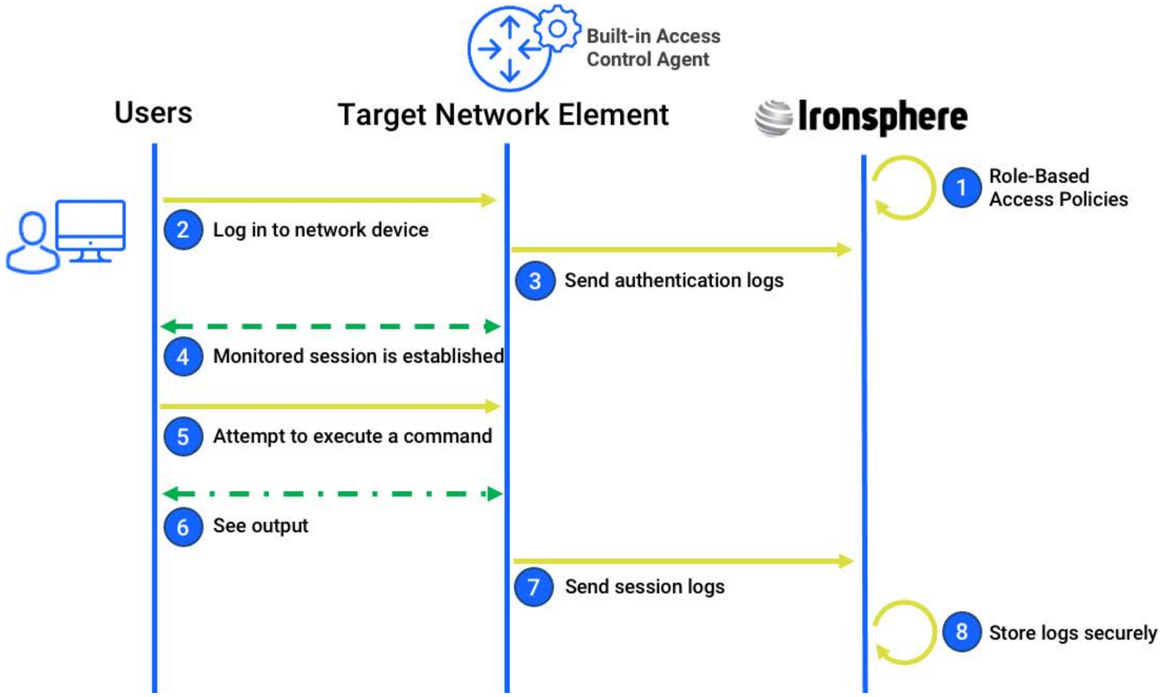
Built-in Access Control Agent
Users
Target Network Element
Ironsphere
1 Role-Based Access Policies
2 Log in to network device
3 Send authentication logs
4 Monitored session is established
5 Attempt to execute a command
6 See output
7 Send session logs
8 Store logs securely

*Figure 5 — Log Management Flow*

**Role-Based Access Policies:** Access policies regarding which users have direct access to which network element, and are allowed to execute which commands, should be configured properly as a one-off initial setup

**Log In to Network Element:** User attempts to log in to the remote network element from an SSH/Telnet 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 built-in 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 network element is successfully established

**Attempt to Execute a Command:** User attempts to execute a command on the remote network element

**Display Output:** Command is executed on remote network element and the user sees the output of the command

**Send Session Logs:** The built-in 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 built-in 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 network elements with their personal accounts on Active Directory
- Multi-Factor Authentication: additional security layer to ensure the person accessing network element is who they claim to be
- In-Session Least Privilege Management: central management of which users can or cannot execute which commands on remote network elements
- Role-Based Privilege Management
- Unified Visibility and Audit Trails of all user activities during direct access sessions