# Syncrude – Internet DMZ Reverse Proxy (F5 BIG-IP) for VDI access

Documentation to Assist with Handover of

Syncrude Internet DMZ external F5 VDI Reverse Proxy

# 

# Table of Contents

[Syncrude – Internet DMZ Reverse Proxy (F5 BIG-IP) for VDI access 1](#_Toc68611097)

[Table of Contents 2](#_Toc68611098)

[Document Change Control 3](#_Toc68611099)

[1. Introduction 3](#_Toc68611100)

[1.1 Purpose of this document (Goal) 3](#_Toc68611101)

[1.2 Intended Audience 3](#_Toc68611102)

[1.3 ‘VDI Reverse Proxy’ Overview and High Level Design 4](#_Toc68611103)

[1.4 ‘VDI Reverse Proxy’ Network Infrastructure and Low Level Design 5](#_Toc68611104)

[2. Support Handover Information 6](#_Toc68611105)

[2.1 ‘VDI Reverse Proxy’ Virtual Device Information 6](#_Toc68611106)

[2.2 ‘VDI Reverse Proxy’ Software License Information 6](#_Toc68611107)

[2.3 DMZ North and South Firewall Rules for the VDI Reverse Proxy traffic 8](#_Toc68611108)

[2.4 BIG-IP LTM settings/profiles for a VDI site (moose.syncrude.com) 9](#_Toc68611109)

[2.5 BIG-IP APM settings/profiles for a VDI site (moose.syncrude.com) 10](#_Toc68611110)

[2.5.1 Access > Profiles/Policies > Access Profiles (Per-Session Policies) > moose.syncrude.com-access 10](#_Toc68611111)

[2.5.2 Access > Connectivity / VPN > Connectivity > moose.syncrude.com-connectivity: 11](#_Toc68611112)

[2.5.3 Access > Connectivity / VPN > VDI / RDP > VDI > moose.syncrude.com-vdi 11](#_Toc68611113)

[2.6 BIG-IP APM Access Policy Flow for VDI access (Flow with SecureAuth) 12](#_Toc68611114)

## Document Change Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Updated by** | **Date** | **Changes made** |
| 1.0 | Shunichi Mikame | March 23, 2021 | Draft/Initial version |
|  |  |  |  |
|  |  |  |  |

# 1. Introduction

## 1.1 Purpose of this document (Goal)

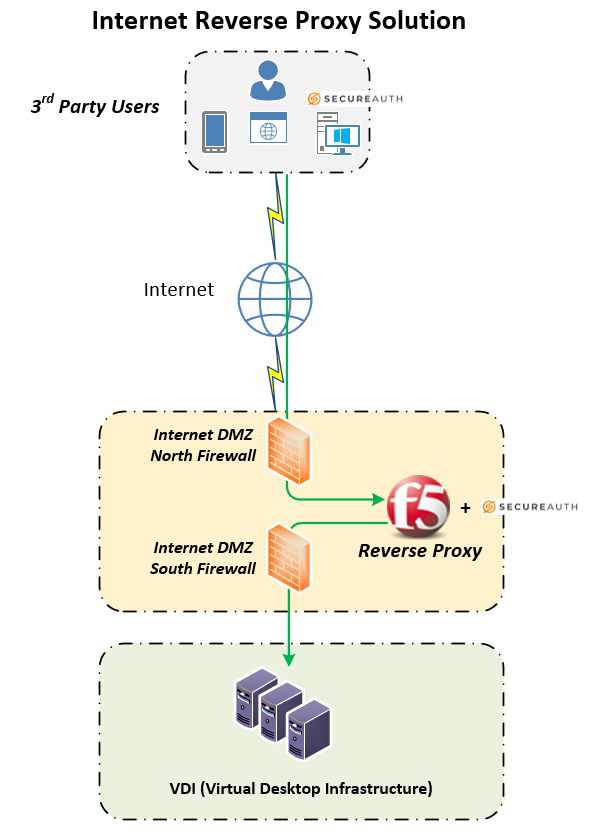
This documentation has been created in order to provide information on the F5 BIG-IP virtual device installed for external user internet, Skype, mobile devices, and Syncrude secure auth access that has been set up as a Reverse Proxy in the Syncrude Internet DMZ environment which will be transitioned to Suncorp.

## 1.2 Intended Audience

This document is intended to be used by IT support staff to help support and migrate the Syncrude Internet DMZ external internet, Skype, mobile devices, and Syncrude secure auth Reverse Proxy (F5 BIG-IP virtual device) used for external user access as needed into their network infrastructure.

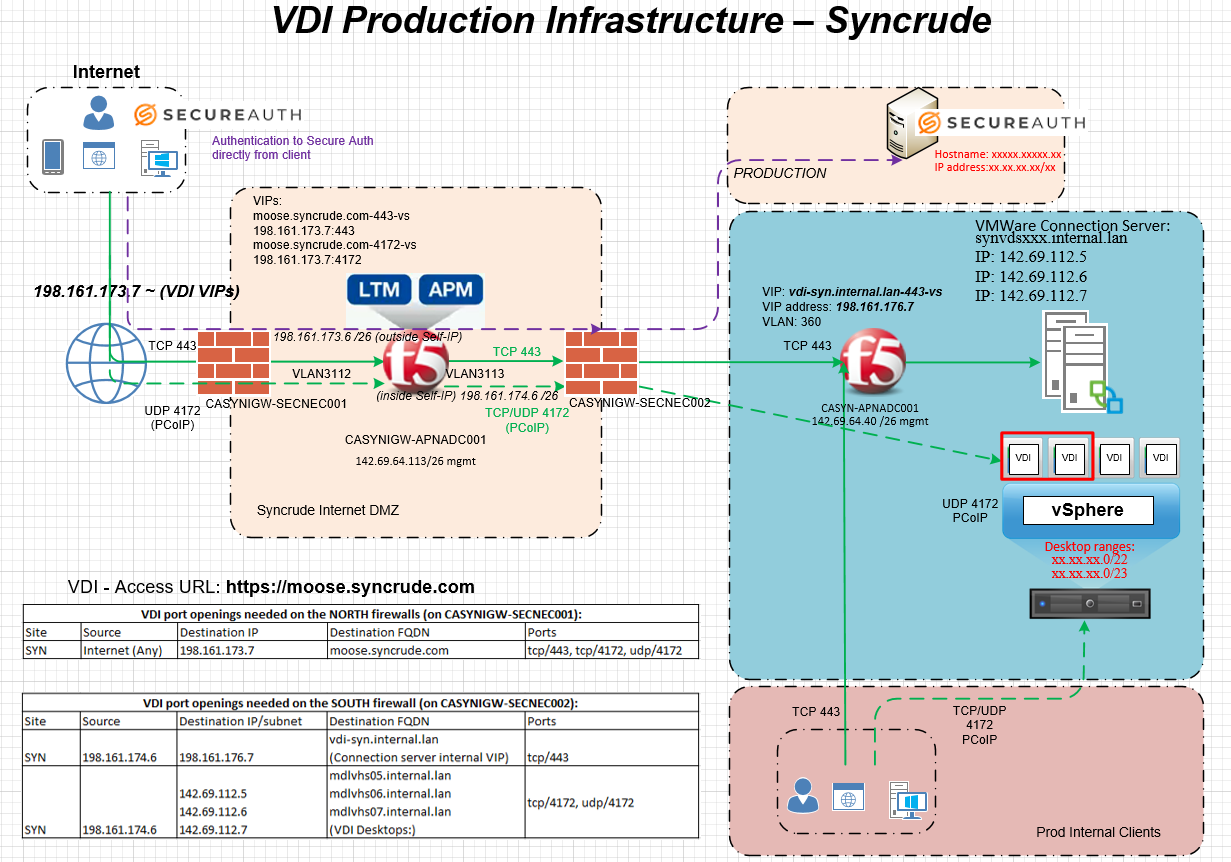
## 1.3 ‘VDI Reverse Proxy’ Overview and High Level Design

VDI access for Syncrude is INBOUND-ONLY access service that Reverse Proxy in DMZ is configured on a standalone F5 BIG-IP 14.1.4 (Virtual Edition) device which is logically hosted on VMware Cluster. The diagrams below describes how VDI Reverse Proxy in Syncrude Internet DMZ was designed in High Level.



## 1.4 ‘VDI Reverse Proxy’ Network Infrastructure and Low Level Design

The diagrams below describes how VDI Reverse Proxy in Syncrude Internet DMZ was designed in Low Level. For a detailed view, please look and refer to the supplemental network design diagram [***Syncrude New DMZ HL and LL Design***](https://ishareteam1.na.xom.com/sites/FIGATEWAY/Transport/Connectivity/Syncrude%20New%20DMZ%20HL%20and%20LL%20Design.vsd) *in Visio format* (see ‘***VDI Design***’ tab).



# 2. Support Handover Information

## 2.1 ‘VDI Reverse Proxy’ Virtual Device Information

**Hardware:**

* N/A

**Software:**

* BIG-IP 14.1.4 (Virtual Edition) Build 0.120.11 Engineering Hotfix
* Chassis Serial Number: 4208d2f9-951e-e9d3-c63ac19bf380

**VM Build info:**

* 3G VE (LTM & APM) = 8 Cores (CPU Count 8) w/16 GB of memory w/80 GB storage

**Hostname:**

* CASYNIGW-APNADC001

**Management and Self-IP Interface IP Addresses:**

* Internet-Facing (“outside”) Interface (Self-IP): 198.161.173.6/26
* Internal-Facing (“inside”) Interface (Self-IP): 198.161.174.6/26
* Management Interface (“management”) Interface: 142.69.64.236 /26

**North VIP Pool and Public FQDN:**

* 198.161.173.7 (FQDN: moose.syncrude.com - VDI Reverse Proxy)
* 198.161.173.8-198.161.173.63 (available for future VIPs)

**VDI User Authentication Method:**

* SecureAuth (an external dependency) as ‘Identify provider’. F5 is ‘Service provider’.

**Routing:**

* No dynamic routing enabled
* Static routes are used for all routing
* Default route is pointed out the internet-facing interface
* Specific routes are pointed to the internal-facing interface

**Device Support Access:**

- Web GUI interface

- CLI via SSH

## 2.2 ‘VDI Reverse Proxy’ Software License Information

**The Sales Order Number:**

- 3955501

**License/ Registration keys for BIG-IP VE keys for sales order 3955501:**

PO Number - 3955501

Line #1 - F5-ADD-BIG-APM-VE-3G Qty : 1

---------------------------------------------

UHUBFIL-ETDKHLP

---------------------------------------------

PO Number - 3955501

Line #2 - F5-BIG-LTM-VE-3G-V18 Qty : 1

---------------------------------------------

OWOZN-GFZTT-JZCAD-ULFXS-RGLXUXX

---------------------------------------------

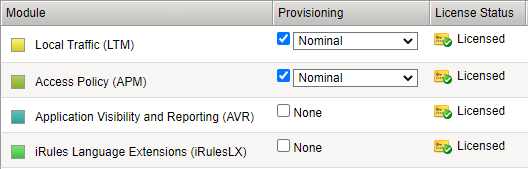
PO Number - 3955501

Line #3 - F5-BIG-LTM-VE-1G-V18 Qty : 1

---------------------------------------------

CKJUF-BDTSZ-KWNSH-AQUDE-NVMRPQI

**Current License status on active modules:**



## 2.3 DMZ North and South Firewall Rules for the VDI Reverse Proxy traffic

There are rules required on the DMZ North and South firewalls that sit in front of BIG-IP Reverse Proxy device facing the Internet as well as the firewall that sits after this device towards the Syncrude internal network. These rules are defined as follows:

**Internet-facing (“North”) Firewall Rules for VDI Reverse Proxy access:**

Rule#1 to Allow Internet to Connect to VDI site (to North Float VIP of F5 VDI Reverse Proxy).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VDI port openings needed on the NORTH firewall (CASYNIGW-SECNEC001):** | | | | |
| **Site:** | **Source IP:** | **Destination IP:** | **Destination FQDN:** | **Ports:** |
| *SYN* | *Internet (Any)* | *198.161.173.7* | *moose.syncrude.com* | *tcp/443 (https \*), udp/tcp-4172 (PCoIP \*)* |

*\* https: uses TCP 443 for Client Authentication*

*\* PC over IP (PCoIP) is a remote display protocol: tcp/4172 is used for session establishment, udp/4172 is used for session data.*

**Internal-facing (“South”) Firewall Rules for VDI Reverse Proxy access:**

Rule#1 to Allow Reverse Proxy connection to an internal F5 loadbalancer VIP for VDI connection server:

Rule#2 to Allow Reverse Proxy south connection (with ‘Auto Map’ option) to VDI Desktop subnets/servers.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VDI port openings needed on the SOUTH firewall (CASYNIGW-SECNEC002):** | | | | |
| **Site:** | **Source IP:** | **Destination IP:** | **Destination FQDN:** | **Ports:** |
| *SYN* | *198.161.174.6* | *198.161.176.7* | *vdi-syn.internal.lan*  *(Connection server internal VIP)* | *tcp/443 (https \*),* |
| *SYN* | *198.161.174.6* | *142.69.112.5*  *142.69.112.6*  *142.69.112.7* | *mdlvhs05.internal.lan*  *mdlvhs06.internal.lan*  *mdlvhs07.internal.lan* | *udp/tcp-4172 (PCoIP \*)* |

*\* https: uses TCP 443 for Client Authentication*

*\* PC over IP (PCoIP) is a remote display protocol: tcp/4172 is used for session establishment, udp/4172 is used for session data.*

## 2.4 BIG-IP LTM settings/profiles for a VDI site (moose.syncrude.com)

The following LTM settings (VIP, Pool, Node, and Monitor) and profiles (TCP Protocol profile, SSL Client profile, and SSL Server profile) have been created and applied on standalone F5 BIG-IP (Virtual Edition) device CASYNIGW-APNADC001 for a VDI site moose.syncrude.com.

By navigating CASYNIGW-APNADC001’s web mgmt interface at ‘**Local Traffic > Virtual Servers > Virtual Server List**’ (and also at **> Pools**, **> Nodes**, and **> Monitors**), you can view how each Virtual Server was configured and tied with what Pool and Node and also can view how ‘**SSL client/server profiles**’, ‘**Access profile’**, ‘**Connectivity profile**’, and ‘**VDI profile**’ are associated/mapped with a virtual server.

**Local Traffic > Virtual Servers > Virtual Server List:**

|  |  |  |
| --- | --- | --- |
| **LT > Virtual Servers:** | **> Virtual Server List:** | |
| **moose.syncrude.com-4172-vs:**          ***Also look the following config items/profiles:***  *LT > Virtual Serv > Pools > Pool List >* ***moose.syncrude.com-443-pl***  *LT > Virtual Serv > Nodes > Node List > <****Node\_IP\_Address****>*  *LT > Monitors > Monitor List >* ***https-vdi-connection\_manager-syn***  *LT > VS > Profiles > Protocol > TCP >* ***tcp-wan-optimized-moose.syncrude.com***  *LT > Virtual Serv > Profiles > SSL > Client* ***> clientssl-moose.syncrude.com***  *LT > Virtual Serv > Profiles > SSL > Server >* ***serverssl-moose.syncrude.com***  *Access > Profiles/Policies > Access Profiles >* ***moose.syncrude.com-access***  *Access > Connectivity/VPN > Connectivity >* ***moose.syncrude.com-connectivity***  *Access > Connectivity/VPN > VDI/RDP > VDI Profiles >* ***moose.syncrude.com-vdi***  *Access > Conn / VPN > VDI / RDP >* ***moose.syncrude.com\_remote\_desktop***  *Access > Conn / VPN > VDI / RDP >* ***moose.syncrude.com\_SAML\_remote\_desktop*** | **moose.syncrude.com-443-vs:** |

## 2.5 BIG-IP APM settings/profiles for a VDI site ([ext-mail.syncrude.com-443-vs\_combined\_https](https://casynigw-apnadc001/tmui/Control/jspmap/tmui/locallb/virtual_server/properties.jsp?name=/Common/ext-mail.syncrude.com-443-vs.app/ext-mail.syncrude.com-443-vs_combined_https))

The following APM settings/profiles have been created and applied on a standalone F5 BIG-IP 14.1.4 (Virtual Edition) device CASYNIGW-APNADC001 for a VDI site moose.syncrude.com.

By navigating CASYNIGW-APNADC001’s web mgmt interface at ‘**Access > Profiles / Policies**’ (and also at ‘**Access > Authentication’**, and **‘Access > Connectivity**’), you can view how each profile was configured and associated with what virtual server.

|  |  |  |
| --- | --- | --- |
| **Profile or Policy Name:** | **Description:** | **Mapped to Virtual servers:** |
| ***Access profile:***  [***ext-mail.syncrude.com-access***](https://casynigw-apnadc001/tmui/Control/jspmap/tmui/accessctrl/profiles/properties.jsp?name=/Common/ext-mail.syncrude.com-access)  ***Access Policy (Per-Session Policy): /Common/***[***ext-mail.syncrude.com-access***](https://casynigw-apnadc001/tmui/Control/jspmap/tmui/accessctrl/profiles/properties.jsp?name=/Common/ext-mail.syncrude.com-access) | *An* ***access profile*** *is to provide the access policy configuration for a virtual server that establishes a secured session. It is a set of group settings that you can use to configure secure Network Access for an application.*  *An* ***access policy*** *(Per-Session Policy) is to provide authentication, endpoint checks, and resources for an access profile. It adds a logon page, gets user credentials, submits them to an authentication type of our choice, then allows authenticated users, and denies others. With the Visual Policy Editor, you can add actions/macros and authentication server object/pool to a policy in a visual flow.* | [ext-mail.syncrude.com-443-vs\_combined\_https](https://casynigw-apnadc001/tmui/Control/jspmap/tmui/locallb/virtual_server/properties.jsp?name=/Common/ext-mail.syncrude.com-443-vs.app/ext-mail.syncrude.com-443-vs_combined_https) |

For configuration details, please look the section 2.5.1, 2.5.2, and 2.5.3 for Access Profile, Connectivity profile, and VDI profile.

### 2.5.1 Access > Profiles/Policies > Access Profiles (Per-Session Policies) > moose.syncrude.com-access

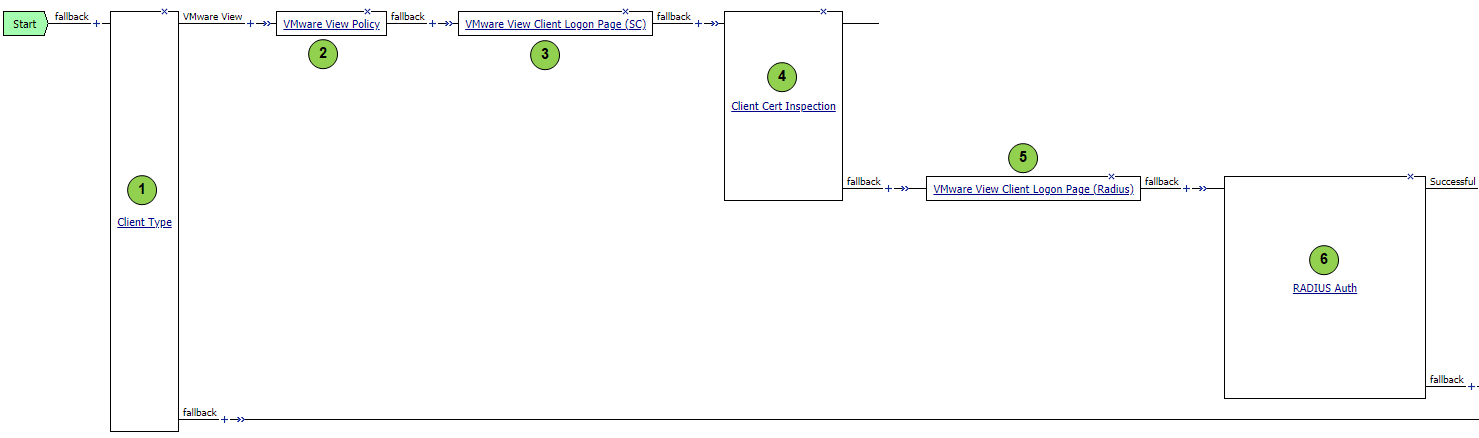
*An* ***access profile*** *is to provide the access policy (a set of group setting for network access) for a virtual server. An* ***access policy (Per-Session Policy)*** *is to provide authentication, endpoint checks, and resources for an access profile. It adds a logon page, gets user credentials, submits them to an authentication type of our choice, then allows authenticated users, and denies others. The policy flow can be created, edied, and displayed visually by using ‘Visual Policy Editor’.*

|  |  |  |
| --- | --- | --- |
| **Access > Profiles/Policies:** | **> Access Profiles (Per-Session Policies):** | |
| [***ext-mail.syncrude.com-access***](https://casynigw-apnadc001/tmui/Control/jspmap/tmui/accessctrl/profiles/properties.jsp?name=/Common/ext-mail.syncrude.com-access)**:** | [**ext-mail.syncrude.com-443-vs\_combined\_https**](https://casynigw-apnadc001/tmui/Control/jspmap/tmui/locallb/virtual_server/properties.jsp?name=/Common/ext-mail.syncrude.com-443-vs.app/ext-mail.syncrude.com-443-vs_combined_https)**:**  **(See LTM Virtual Server setting section/page)**  [debug\_activesync\_email](https://casynigw-apnadc001/tmui/tmui/util/ajax/app-shim.jsp?appId=apps.AccessPolicy.apmLogProfile&editButtonId=editLogProfile&gridId=apmlogprofile&selectAttributeKey=name&selectAttributeValue=/Common/debug_activesync_email)**:**    **Per-Session Policy (use Visual Policy Editor):**  **Click ‘Edit’ for viewing/editing ‘Access Policy’.** |

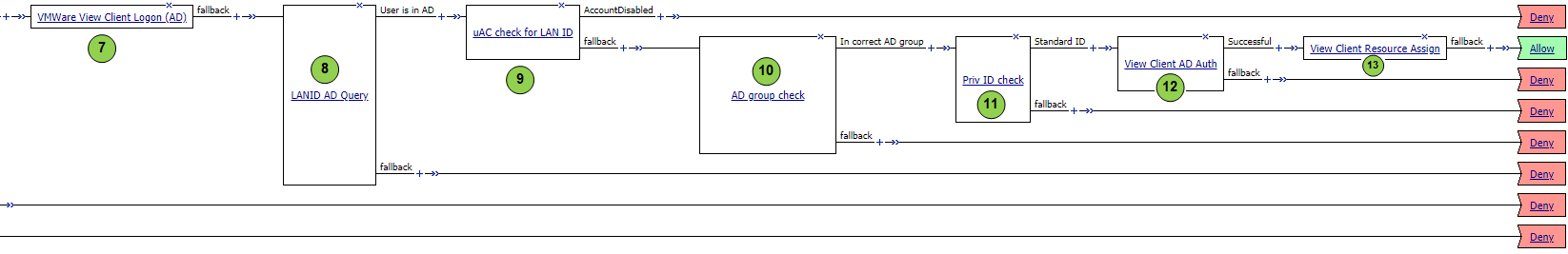
## 2.6 BIG-IP APM Access Policy Flow for VDI access (Flow with SecureAuth)

An **access policy** is to provide authentication, endpoint checks, and resources for an access profile. It adds a logon page, gets user credentials, submits them to an authentication type of our choice, then allows authenticated users, and denies others. With the ‘Visual Policy Editor’, you can add items to a policy in a visual flow, using predefined actions and macros. You can also create your own rules and macros. The following access policy flow has been created for moose.syncrude.com VDI site access.

***Access Policy: /Common/***[***ext-mail.syncrude.com-access***](https://casynigw-apnadc001/tmui/Control/jspmap/tmui/accessctrl/profiles/properties.jsp?name=/Common/ext-mail.syncrude.com-access)



|  |  |  |
| --- | --- | --- |
| **#** | ***Flow Name:*** | ***Description/Purpose:*** |
| **0** | ***Start*** |  |
| **1** | ***Client Type*** | Determines whether the user is connecting via a full or mobile browser, Edge Client, Edge Portal, Machine Tunnel, Citrix Receiver, VMware View, Microsoft RDP client or MS-OFBA Compliant clients. Expression with ‘Client type is VMware View’ is used. |
| **2** | ***VMware View Policy*** | Variable Assign that use this action to specify a policy that enables or disables USB redirection for VMware View connections and can pass Start Session Script Variables to the View Connection Server (VCS). Fallback to next flow. |
| **3** | ***VMware View Client Logon Page (SC)*** | This action creates a VMware View logon page for the policy, and we add this item before an authentication action. Smart Card Displays a VMware View logon screen that requests a PIN. Fallback to next flow. |
| **4** | ***Client Cert Inspection*** | A new Branch Rule with an expression ‘Client Certificate is valid’ |
| **5** | ***VMware View Client Logon Page (Radius)*** | This action creates a VMware View logon page for the policy, and we added this item before an authentication action. RADIUS Displays a VMware View logon screen that requests RADIUS credentials. |
| **6** | ***RADIUS Auth*** | Specifies the RADIUS authentication server object. Use this item to add RADIUS authentication to the policy branch. Select the server from the list (Servers are defined in the Access > Authentication area of the Configuration utility).  The following RADIUS (SecureAuth) server is mapped from this flow.  **/Common/SYN\_SecureAuth** |



|  |  |  |
| --- | --- | --- |
| **#** | ***Flow Name:*** | ***Description/Purpose:*** |
| 7 | ***VMWare View Client Logon (AD)*** | This action creates a VMware View logon page for the policy, and added this item before an authentication action. |
| 8 | ***LANID AD Query*** | The system queries the Active Directory server for the user's attributes.  The following Trusted domain profiles are mapped from this flow.  **/Common/internal.lan** |
| 9 | ***uAC check for LAN ID*** | Message Box that this action creates a message page for the policy and the user sees the message and a prompt to click to continue (a custom message to display to the end user, with prompt to continue). |
| 10 | ***AD group check*** | A new Branch Rule with an expression that user is a member of VDI user group. |
| 11 | ***Priv ID check*** | A new Branch Rule with an expression for checking Standard Accounts. |
| 12 | ***View Client AD Auth*** | Active Directory authentication of end user credentials.Using this item to add Active Directory authentication to the policy branch.  The following Trusted domain profiles are mapped from this flow.  **/Common/internal.lan** |
| 13 | ***View Client Resource Assign*** | Expression-based assignment of Connectivity Resources, Webtop, and ACLs. The following profiles are mapped from this flow.  **Remote Desktop: /Common/moose.symcrude.com\_remote\_desktop**  **Webtop: /Common/ moose.symcrude.com\_webtop** |

---- End of Doc ---