Advanced Technology Group

IBM Storage DS8900F R9.3.2 – What's New!

Brian Sherman, Craig Gordon, John Bernatz, Rick Pekosh – ATG Storage

Accelerate with ATG Technical Webinar Series

Advanced Technology Group experts cover a variety of technical topics.

Audience: Clients who have or are considering acquiring IBM Storage solutions. Business Partners and IBMers are also welcome.

To automatically receive announcements of upcoming Accelerate with IBM Storage webinars, Clients, Business Partners and IBMers are welcome to send an email request to accelerate-join@hursley.ibm.com.

2023 Upcoming Webinars – click on the link to register for the live event:

March 16 - IBM c-type 64G Fabric Switches: Bringing Innovation, Intelligence & Interoperability

March 21 – IBM Storage Ceph 30 Minute Challenge

March 28 - How to Size for FlashSystem Safeguarded Copy 201 – Using IBM Storage Insights to Gather Data

Important Links to bookmark:

ATG Accelerate Support Site: https://www.ibm.com/support/pages/node/1125513

ATG MediaCenter Channel: https://ibm.biz/BdfEgQ

ATG-Storage Offerings

CLIENT WORKSHOPS

- IBM Cloud Object Storage System
- IBM Storage Scale and Storage Scale System
- IBM DS8900F Advanced Functions
- IBM Storage Point of View on Cyber Resiliency
- IBM FlashSystem 9500 Deep Dive & Advanced Functions
- IBM Storage Fusion

Please reach out to your IBM Rep or Business Partner for future dates and to be nominated.

TEST DRIVE / DEMO'S

- North America ATG Storage - IBM Storage Scale and Storage Scale System GUI
- North America ATG Storage - IBM Storage Virtualize Test Drive
- North America ATG Storage - IBM DS8900F Storage Management Test Drive
- North America ATG Storage - Managing Copy Services on the DS8000 Using IBM Copy Services Manager Test Drive
- North America ATG Storage - IBM DS8900F Safeguarded Copy (SGC) Test Drive
- North America ATG Storage - IBM Cloud Object Storage Test Drive - (Appliance based)
- North America ATG Storage - IBM Cloud Object Storage Test Drive - (VMware based)
- North America ATG Storage - IBM Storage Protect Live Test Drive
- North America ATG Storage - IBM Storage Protect Plus Live Test Drive
- North America ATG Storage - IBM Storage Ceph Test Drive - (VMware based)

Please reach out to your IBM Rep or Business Partner for more information.

Accelerate with ATG Technical Webinar Series - Survey

Please take a moment to share your feedback with our team!

You can access this 6-question survey via Menti.com with code 2243 3599 or

Direct link https://www.menti.com/albneqj15g57

Or

QR Code

Advanced Technology Group

IBM Storage DS8900F R9.3.2 – What's New!

Brian Sherman, Craig Gordon, John Bernatz, Rick Pekosh – ATG Storage

Meet the Speakers

Brian Sherman is a Distinguished Engineer with over thirty years experience as a Storage I/T Specialist. Brian works directly with clients WW in solving storage related challenges.
Brian has extensive understanding of storage related industry trends and emerging technologies. He currently provides Storage Hardware and Software technical sales and support as part of the Advanced Technology Group (ATG) organization. Brian also develops and provides World Wide technical education on new Storage Hardware and Software product launches, best practices and provides new function priorities to several Storage Product Development Teams.

Craig Gordon is a Senior Brand Technical Specialist currently working in the Advanced Technology Group (ATG) for Storage. Craig has been supporting sales for IBM's DS8000 product family since it was introduced in 2004 and supported the Enterprise Storage Server, aka Shark, before that time. Craig is a respected subject matter expert in the implementation of DS8000 storage for mainframe and open systems platforms, to include Copy Services deployments, sizings, and data migration planning.

John Bernatz is a Senior Brand Technical Specialist with the IBM Advanced Technology Group. John has extensive experience in working with most products in the IBM storage portfolio and is an expert in Open Systems attachment and management and IBM's zLinux solutions.

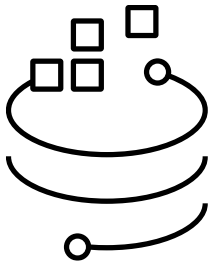
Rick Pekosh is a Senior Brand Technical Specialist working in the IBM Advanced Technology Group as a DS8000 subject matter expert specializing in High Availability, Disaster Recovery, and Cyber Resiliency solutions. He works with customers, IBM Business Partners, and IBMers in North America. Rick began working with the DS8000 in early 2005 while working as a technical sales specialist and functioning as a regional designated specialist. He joined IBM in 2001 after spending 20 years in application development in various roles for the Bell System and as a consultant. Rick earned a BS degree in Computer Science from Northern Illinois University and an MBA from DePaul University. Additionally, his IBM Profession Certification level is Certified IT Specialist (Expert).

Agenda

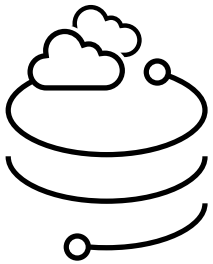
- **IBM Storage Portfolio Announcement Summary – March 2, 2023**
- **Multi-Factor Authentication**
- **Customer Provided Certificates for Call Home**
- **Safeguarded Copy Enhancement**
  - ✓ **Preserve backups**
- **Host Event Notification Improvements**

IBM Storage Portfolio

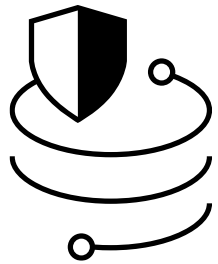
Announced March 2, 2023



Storage for Data and AI



Storage for Hybrid Cloud



Storage for Data Resilience

	Storage for Data and AI	Storage for Hybrid Cloud	Storage for Data Resilience
Software	IBM Storage Scale IBM Storage Ceph	IBM Storage Fusion IBM Storage ODF	IBM Storage Defender IBM Storage Insights
Hardware	IBM Storage Scale System	IBM Storage Fusion HCI System	IBM Storage FlashSystem | DS8000 | Tape | Networking

https://www.ibm.com/products/storage-defender

Multi-Factor Authentication

What is MFA & How does it work?

What is Multi-Factor Authentication (MFA)?

An authentication method which requires multiple proofs of identification in order to gain access

A strong method of authentication necessary to protect sensitive data

Factors of Authentication

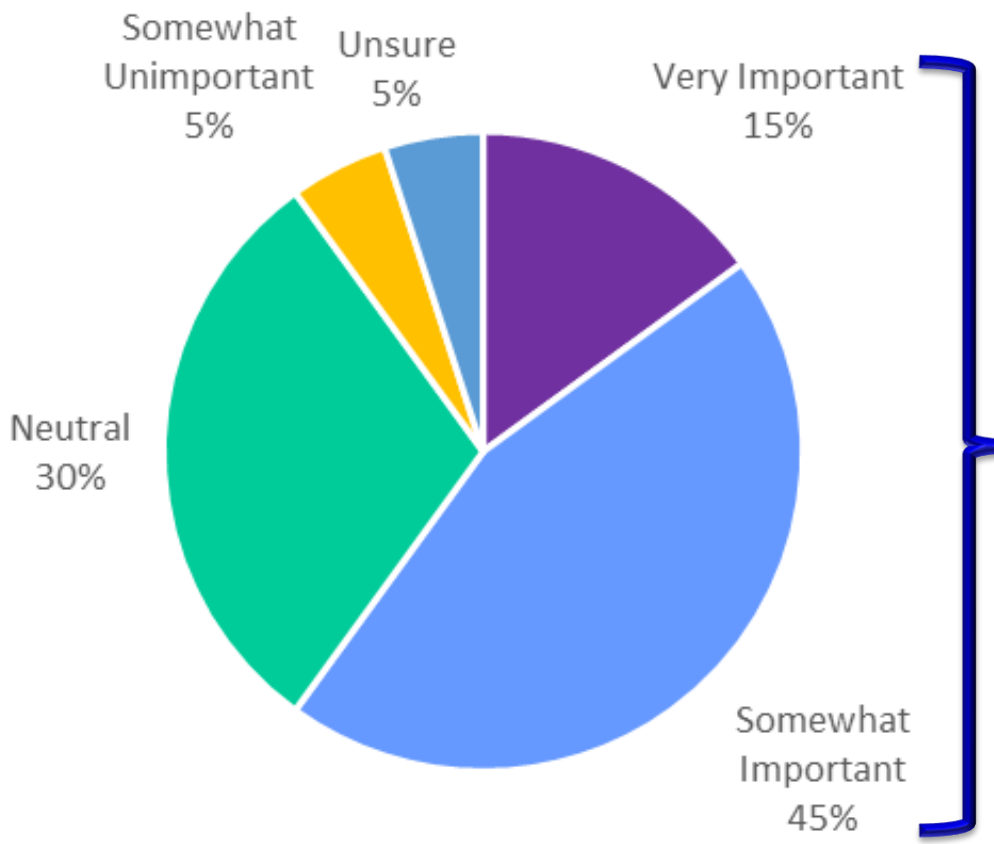
Factors of Authentication

- A factor is a proof of identification
- Some common factors are:
  - ✓ Permanent Passwords
  - ✓ One-Time Passwords delivered by text, phone, or email
  - ✓ Certificates
  - ✓ Tokens
  - ✓ Smart Cards
  - ✓ Key Fobs
  - ✓ Biometrics
- MFA best practices require the following types of factors:
  - ✓ Something you have
  - ✓ Something you know

2022 DS8000 Customer Survey (1 of 2)

2022 DS8000 Customer Survery (1 of 2)

How important is Multi-Factor Authentication?



60% noted that MFA was either *Very Important* or *Somewhat Important*

2022 DS8000 Customer Survey (2 of 2)

2022 DS8000 Customer Survery (2 of 2)

Please rank the following MFA Products from most desirable & feasible to least desirable & feasible

Item	Overall Rank	Overall Score
RSA	1	48
RACF	2	40
IBM Security Verify	3	36
Okta	4	27
PING Identify	5	25
Cisco (Duo)	6	20
Microsoft Azure	7	19
Microsoft FS	8	14
Google	9	14

RSA SecurID Authentication Manager

RSA SecurID Authentication Manager

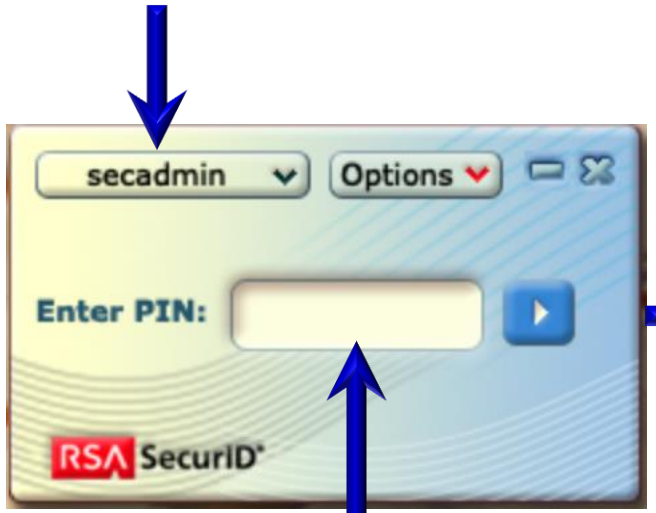
- RSA SecurID Authentication Manger is an On-Premise solution
- DS8000 R9.3.2 communicates with RSA SecurID using RESTful API protocol
- Handles Multi-Factor Authentication
  - ✓ Supports *something you have* – TOKEN
  - ✓ Supports *something you know* – PIN
- Market leader per Gartner
- Most popular MFA server in 2022 DS8000 Customer Survey

RSA SecurID Authentication Manager

RSA Multi-Factor Authentication

- RSA 2-factor authentication requires downloading a TokenID (*something you have*) and entering a PIN (*something you know*)

(security admin gen'd)
Downloaded ***TokenID***

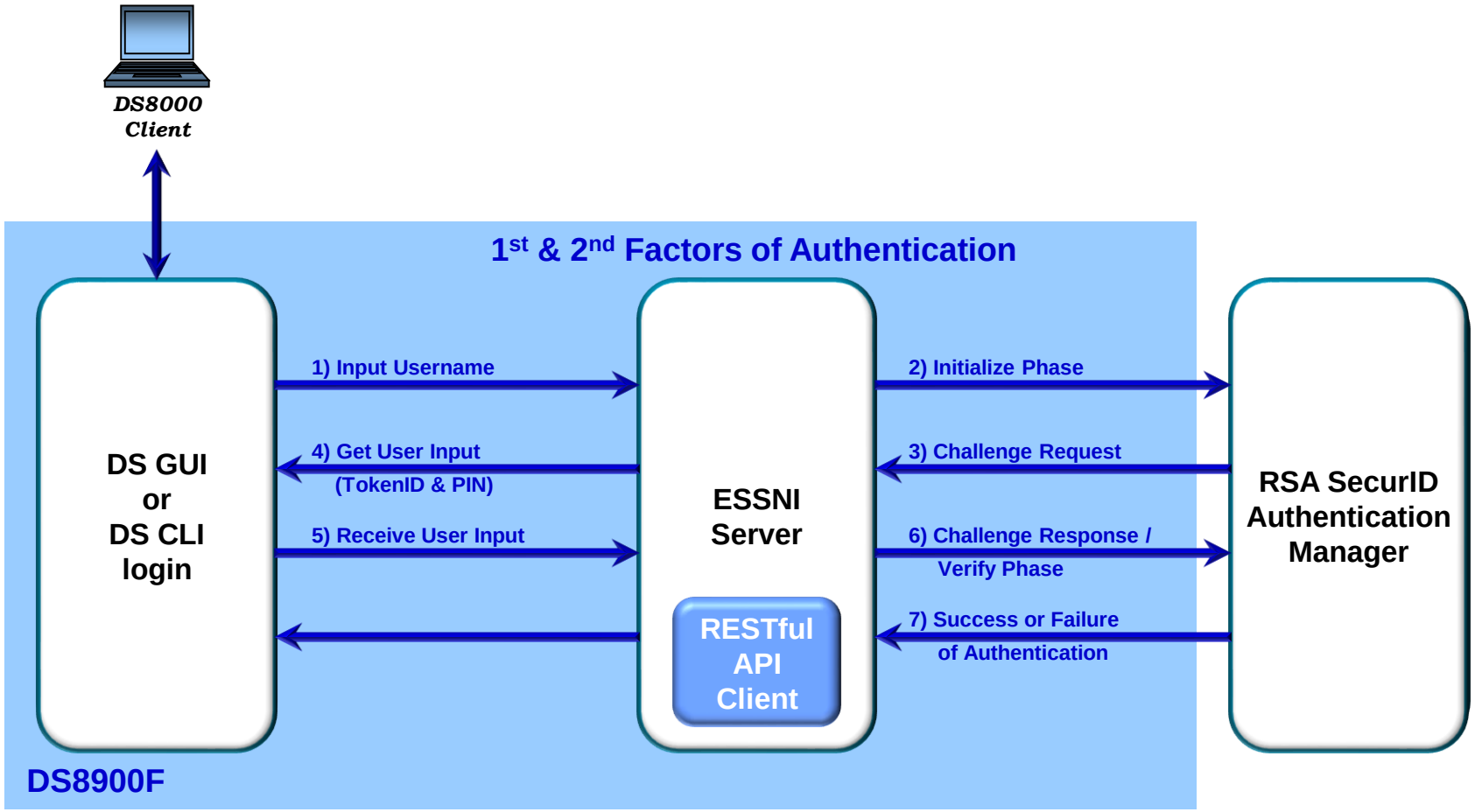


PIN
(user initiated
system gen'd)

(generated single
use time sensitive)
Passcode

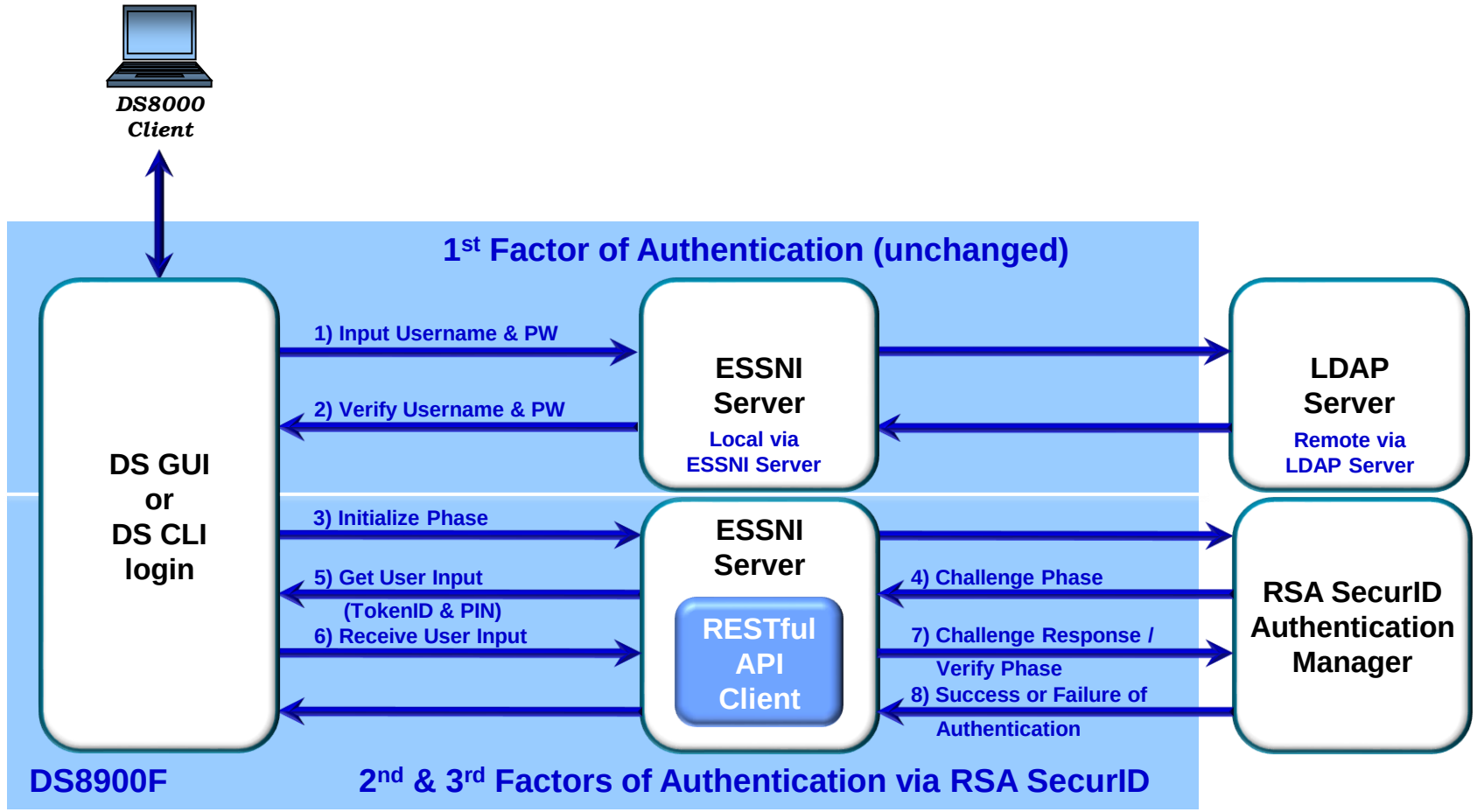
MFA Flow Diagram with all Factors of Authentication Handled by RSA SecurID

MFA Flow Diagram with all Factors of Authentication Handled by RSA SecurID



MFA Flow Diagram with LDAP Server as 1st Factor of Authentication

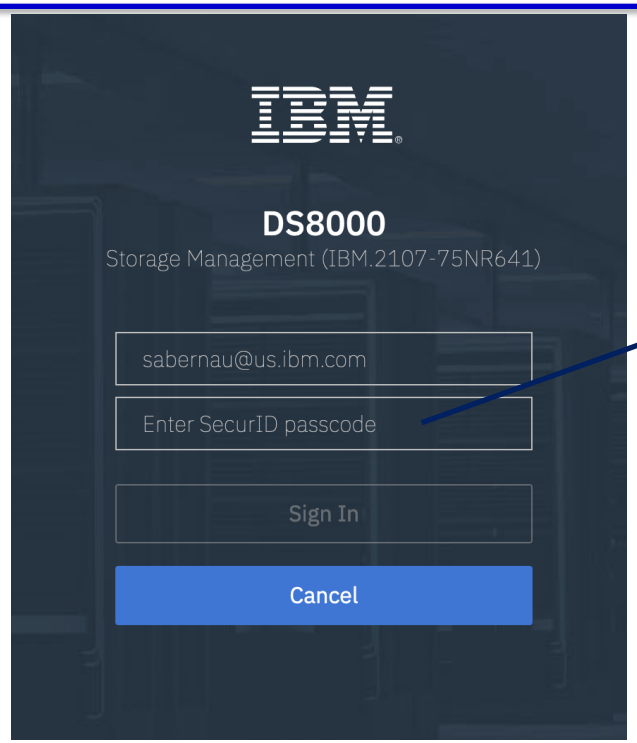
MFA Flow Diagram with LDAP Server as 1st Factor of Authentication



Logging into a DS8000 using MFA

Login using RSA

Login using RSA

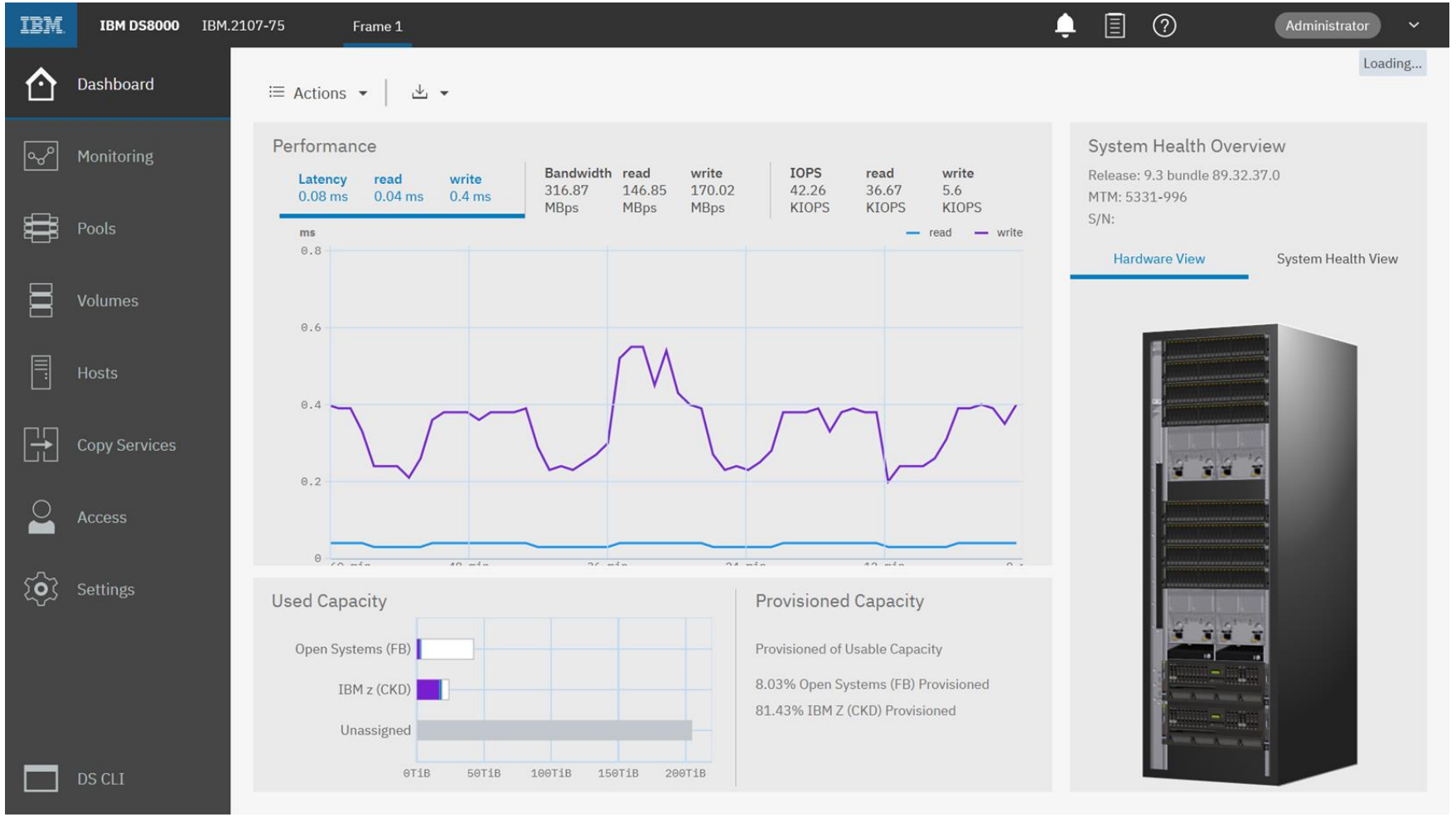


Paste SecurID Passcode Click [Sign In]

Passcode is gen'd Click [Copy]

Login using RSA – Successful login

Login using RSA



Login using RSA + LDAP

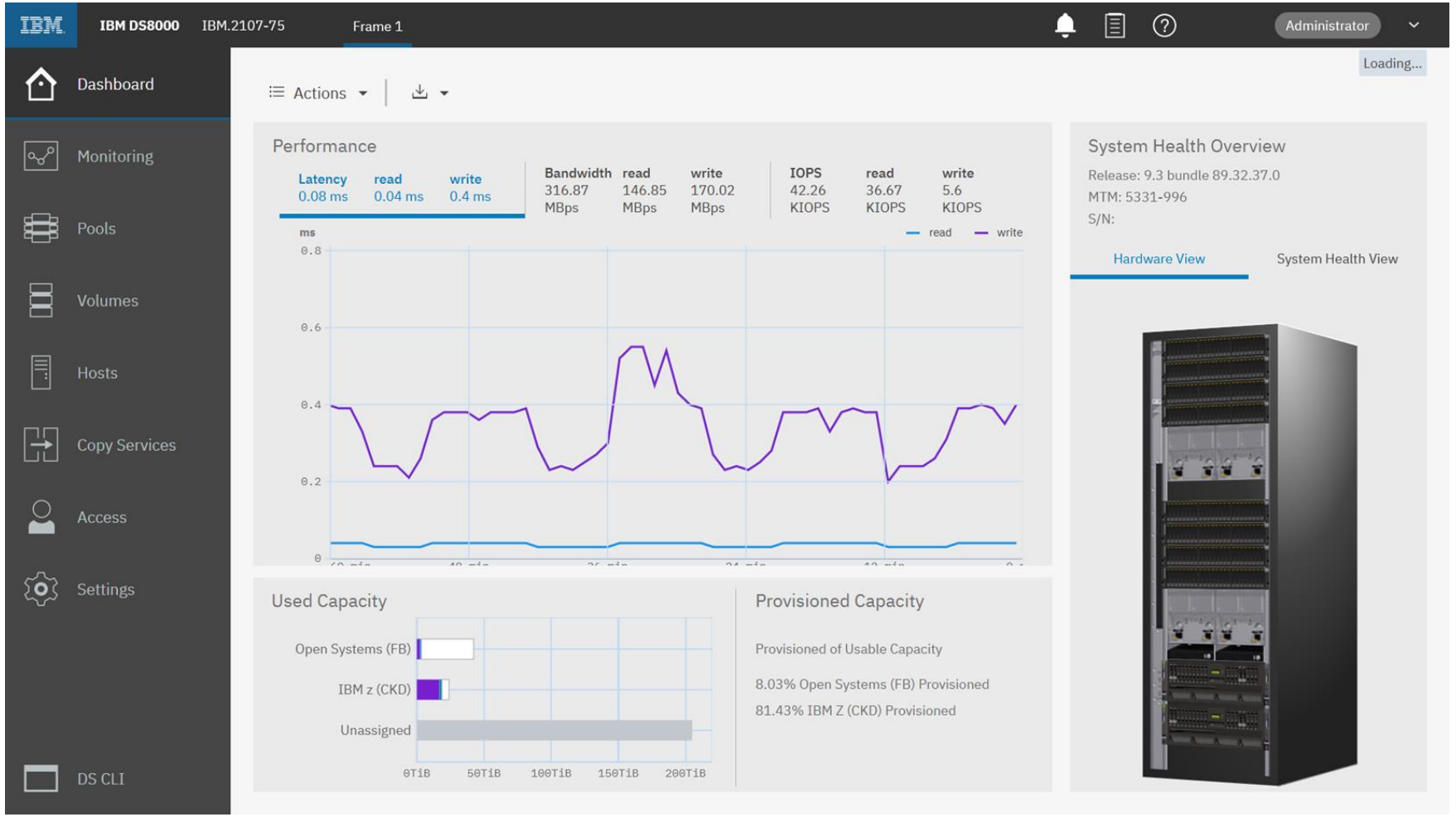
Login using RSA + LDAP

Paste SecurID Passcode Click [Sign In]

Passcode is gen'd Click [Copy]

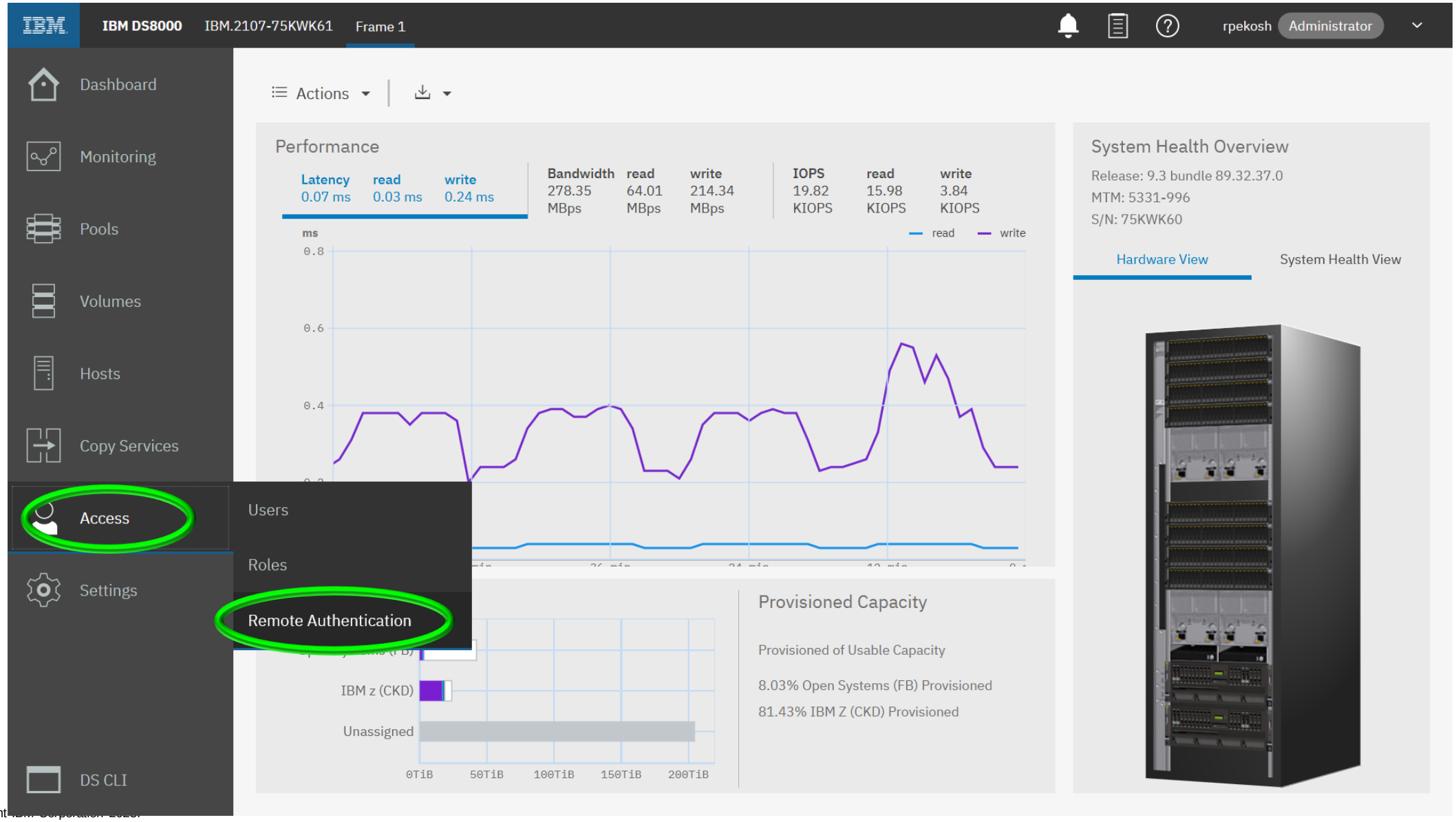
Login using RSA + LDAP – Successful login

Login using RSA + LDAP

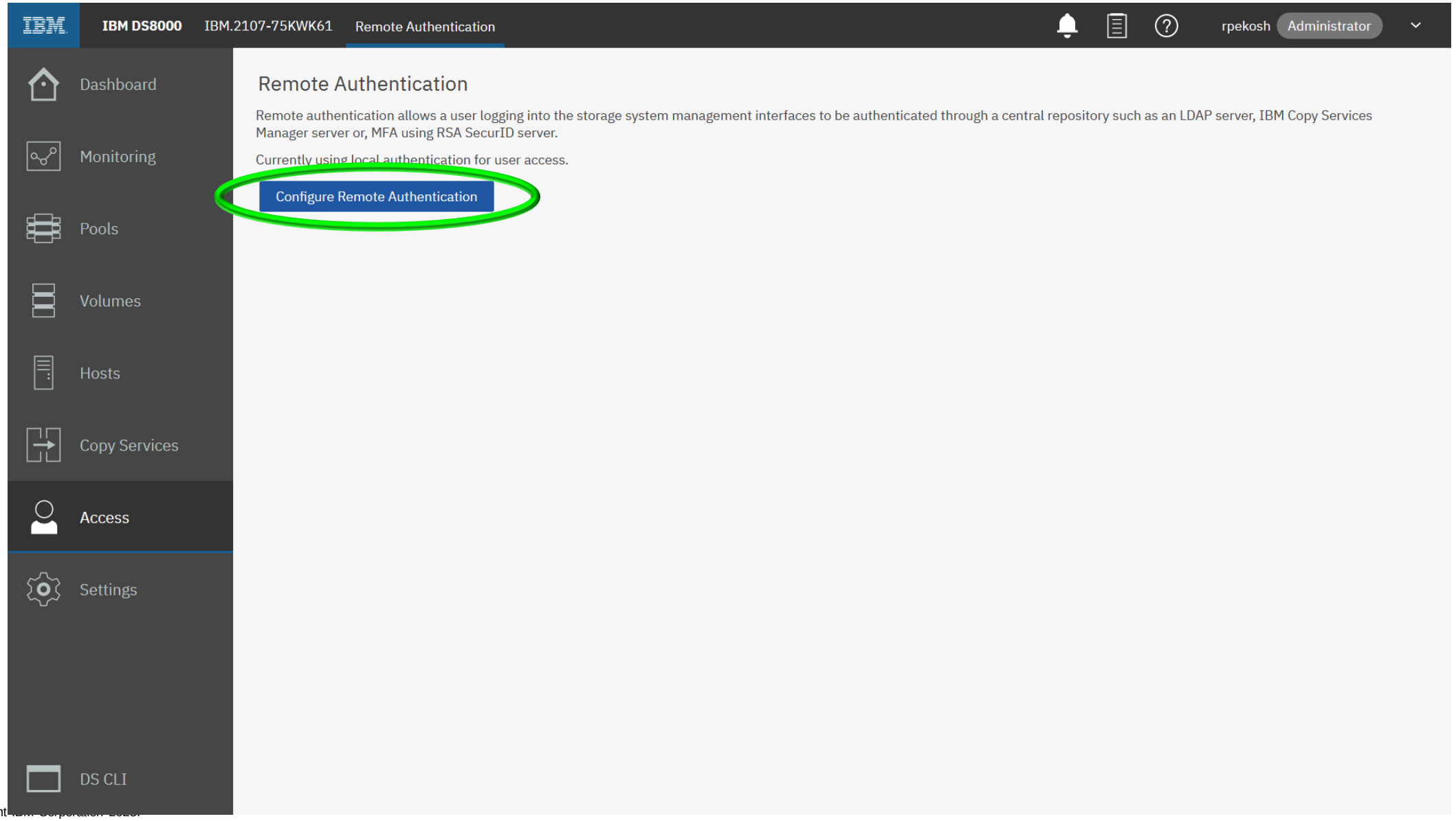


Accessing MFA Setup from the GUI

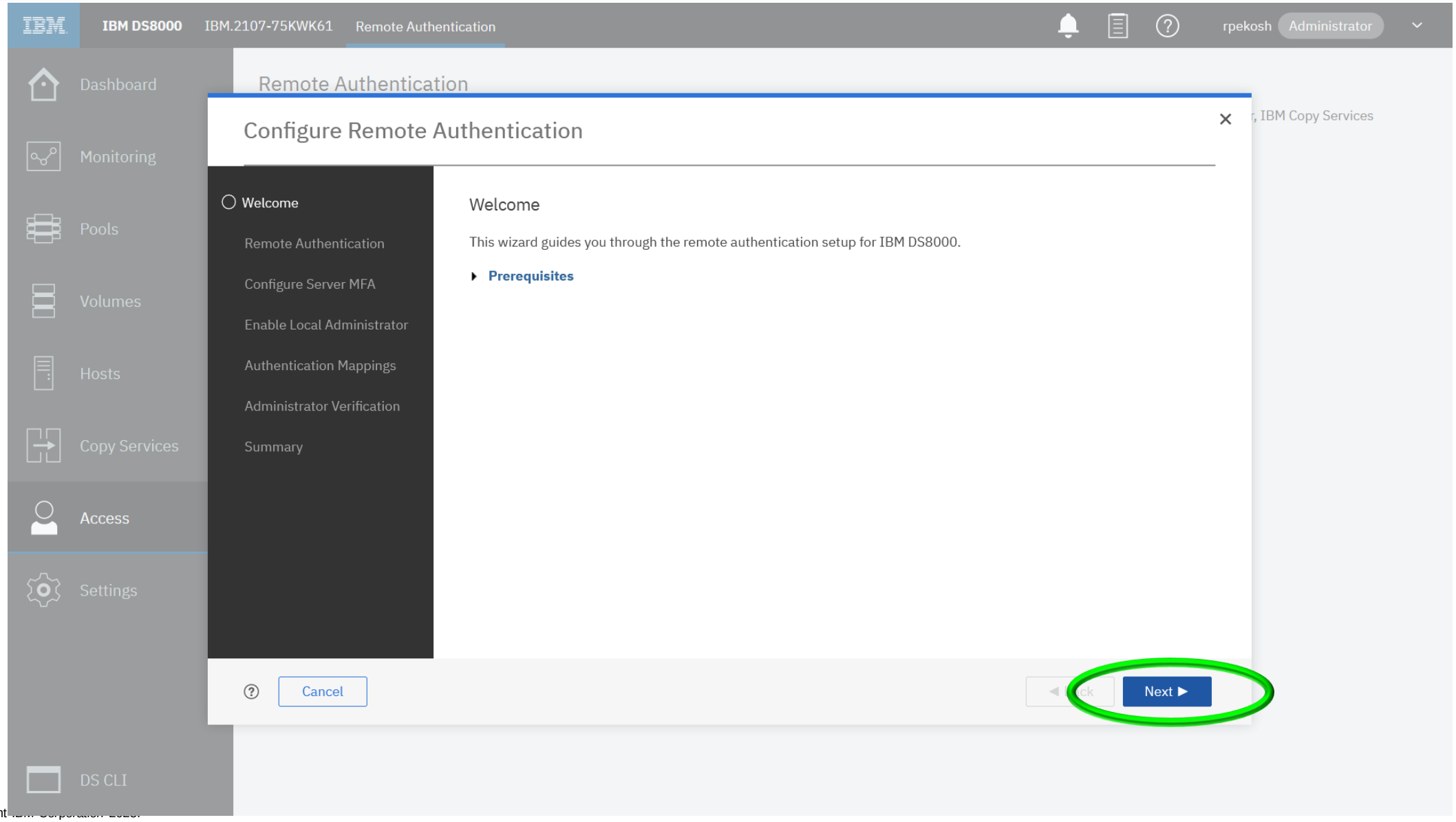
Select *Access → Remote Authentication*



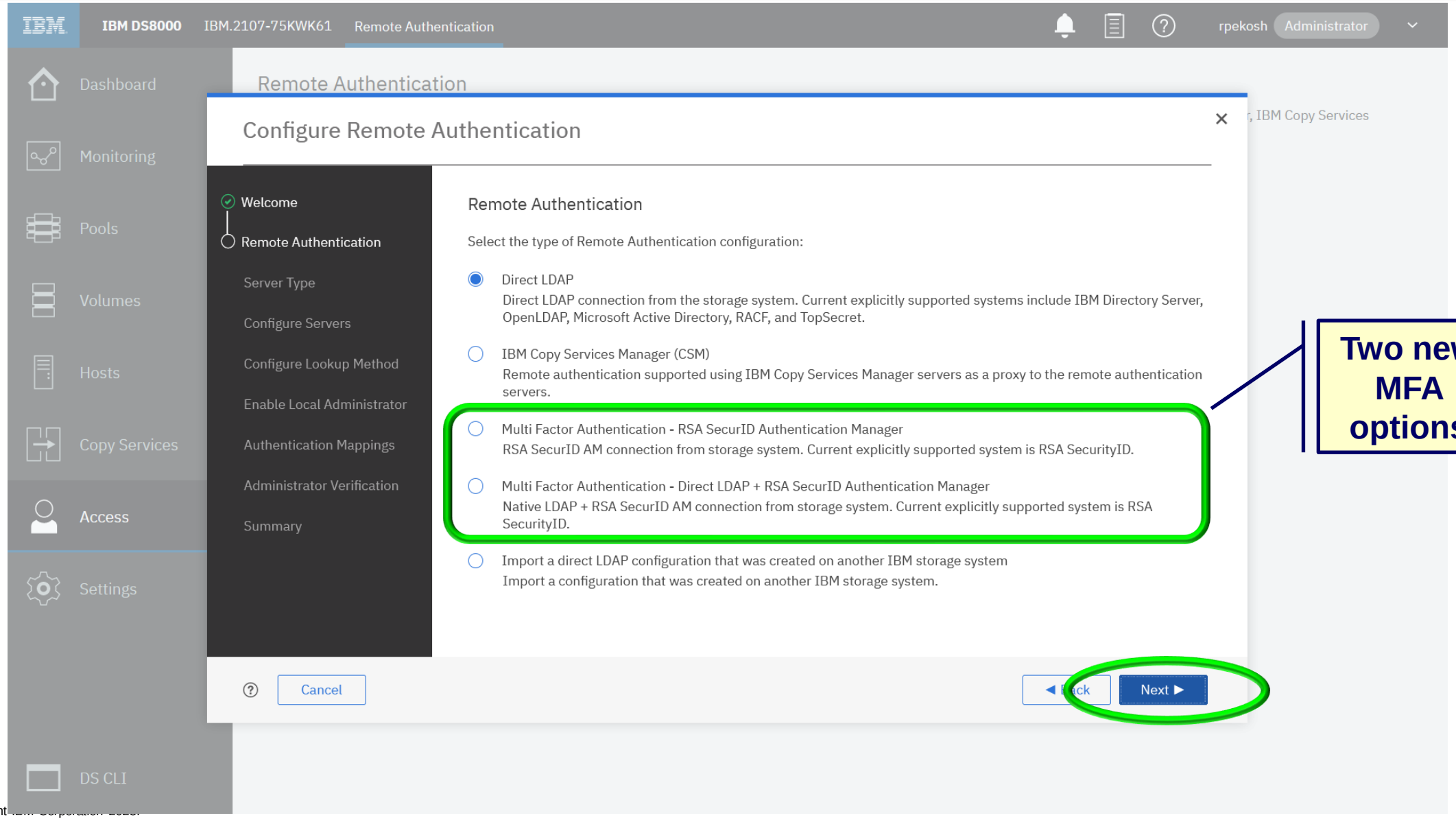
Click *Configure Remote Authentication*



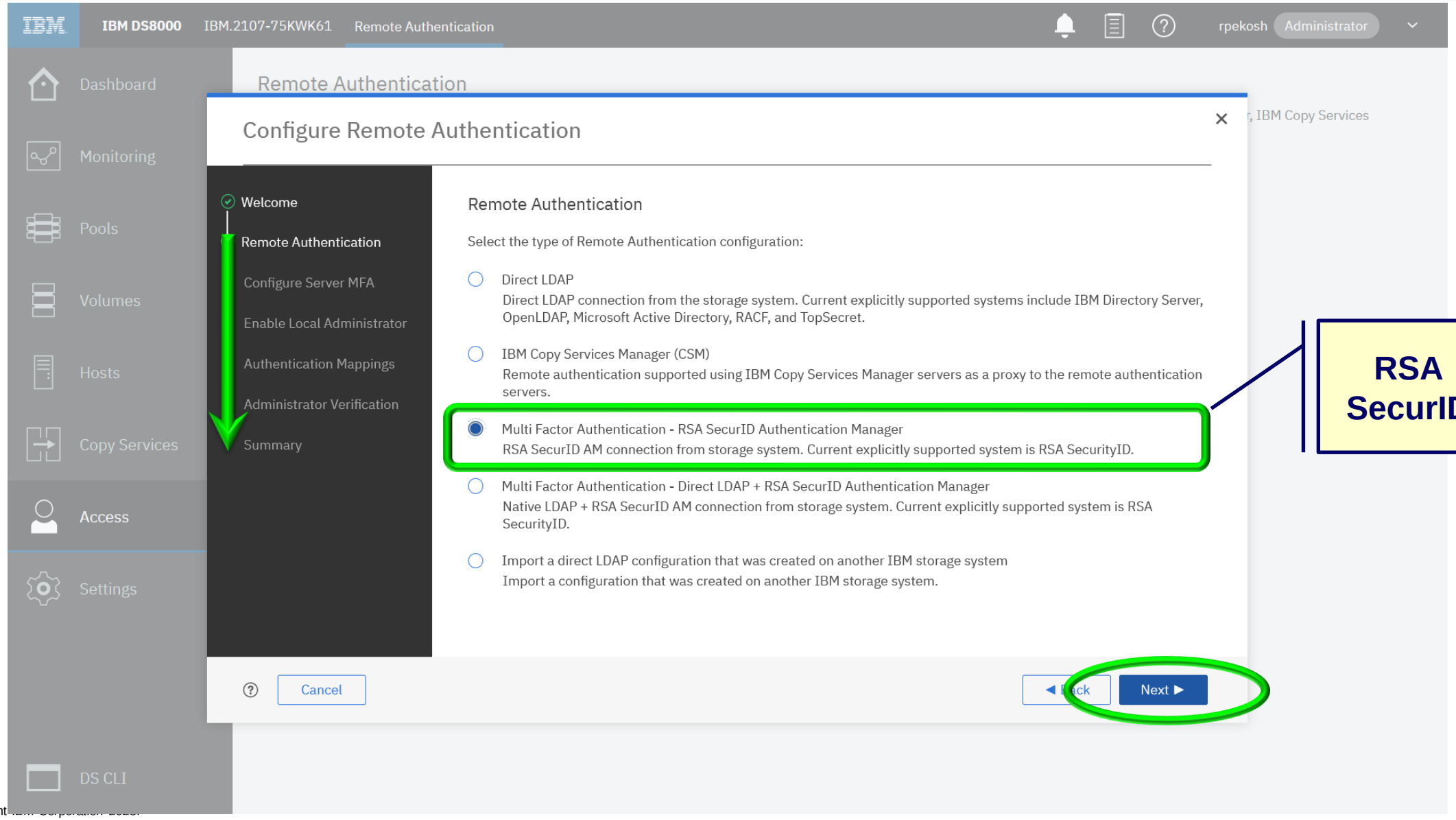
Click *Next*



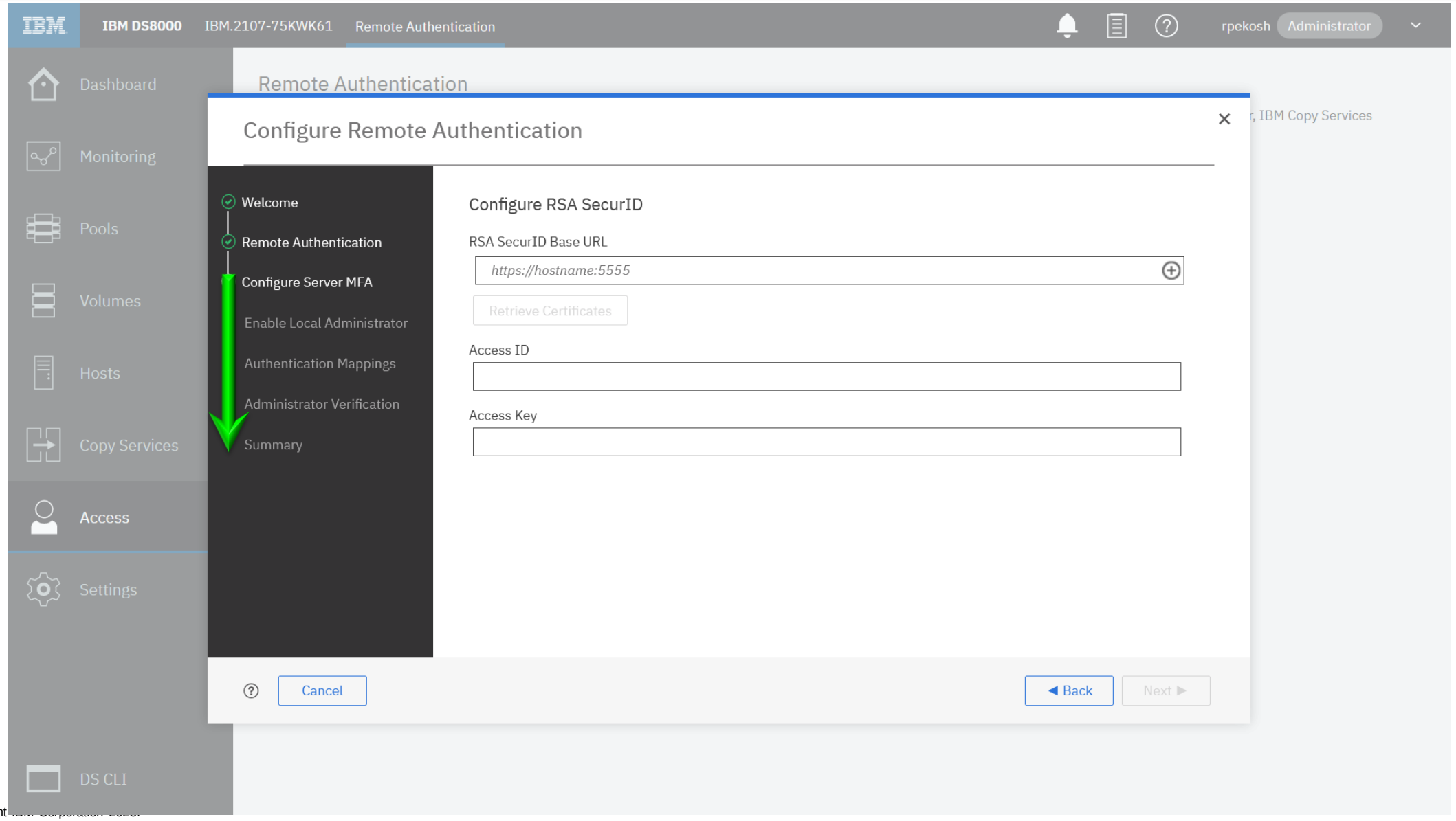
Selecting MFA – RSA SecurID Authentication Manager with & without Direct LDAP



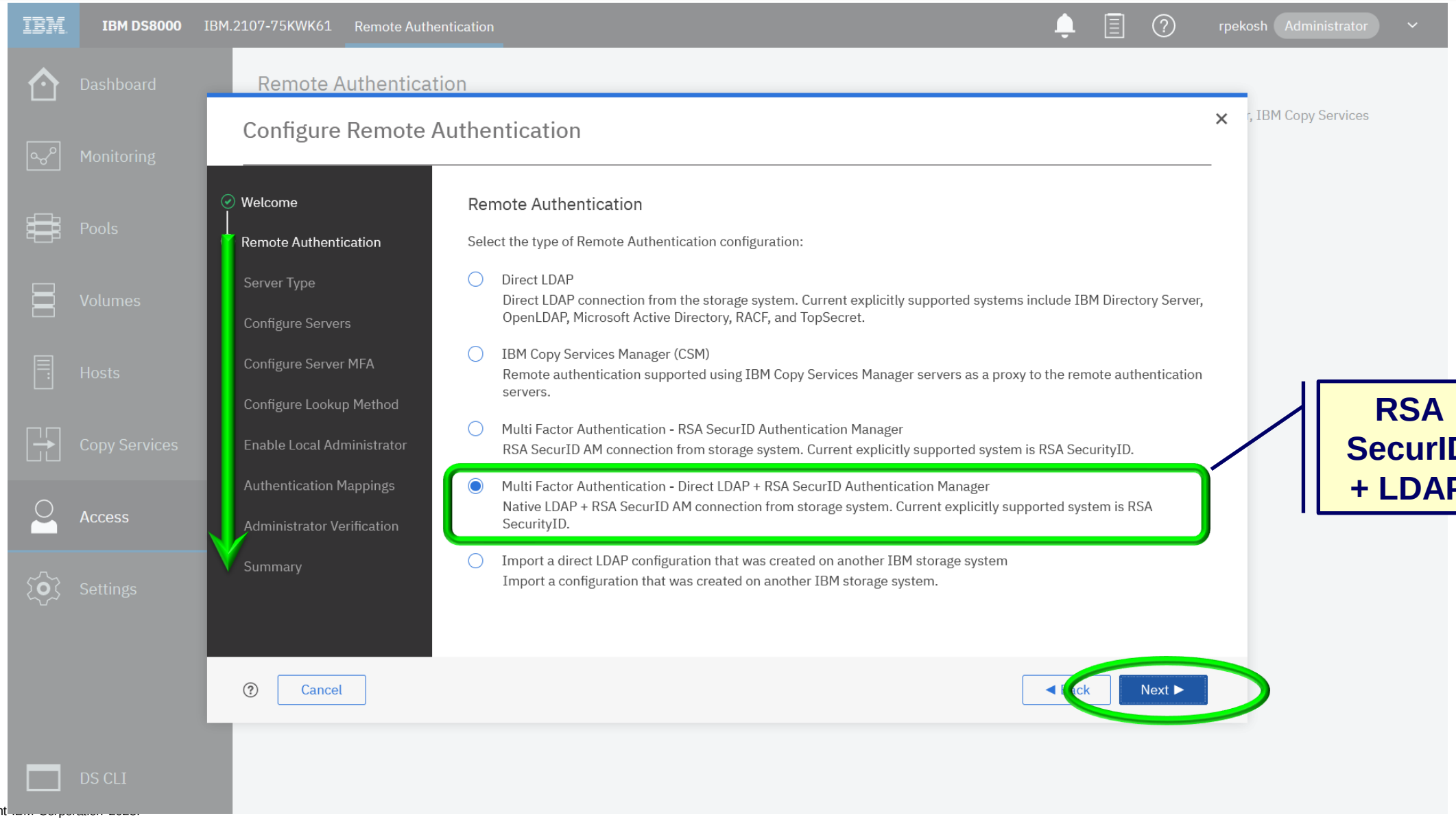
Multi-Factor Authentication – RSA SecurID Authentication Manager



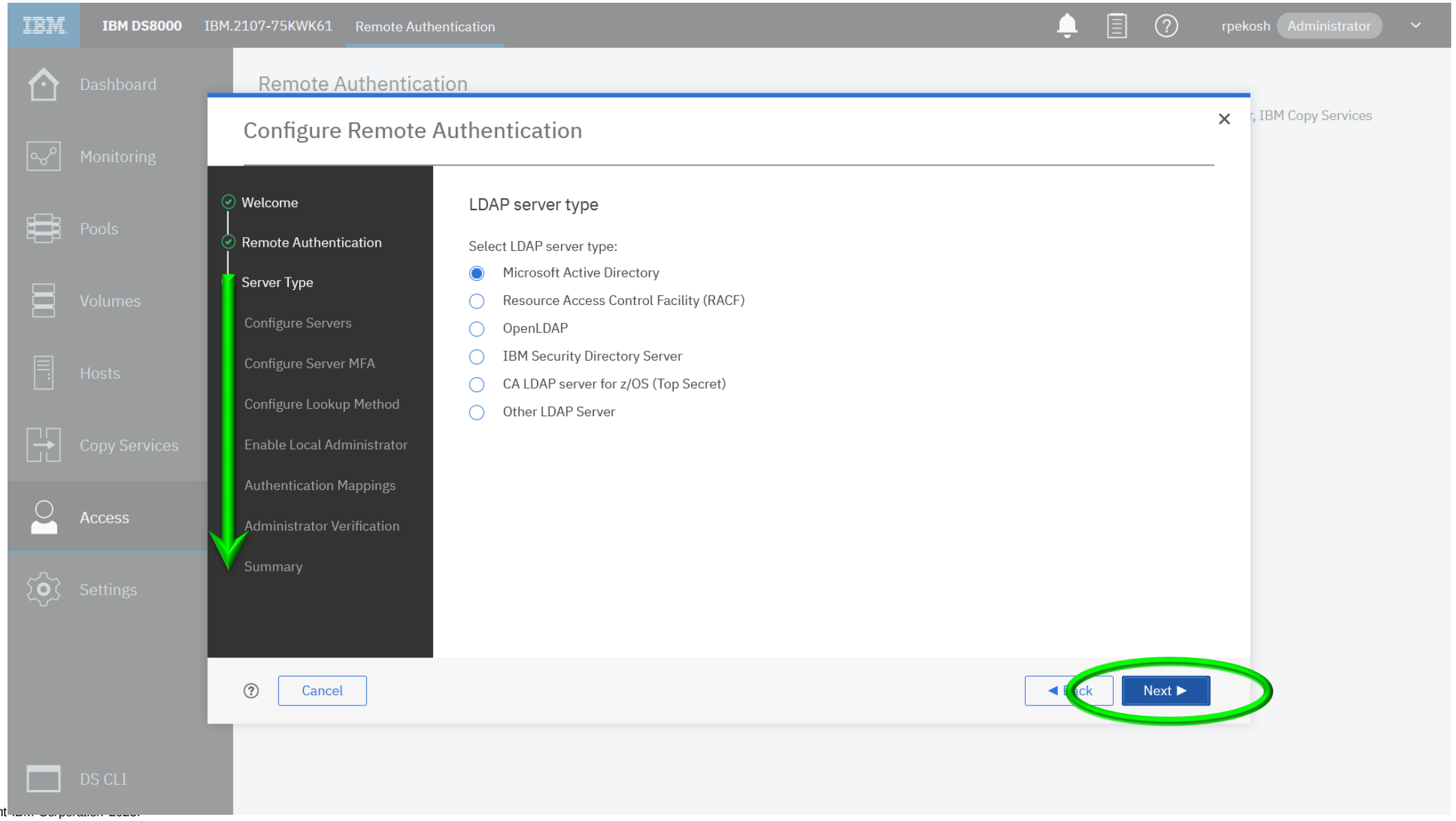
Configure Server MFA



Multi-Factor Authentication – Direct LDPA + RSA SecurID Authentication Manager



Configure Server LDAP + MFA

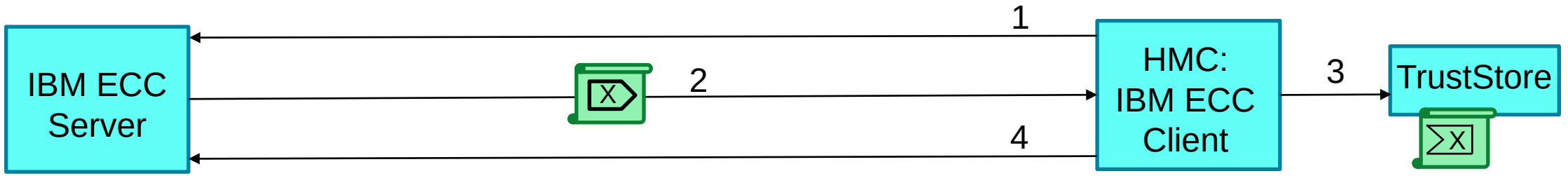


Customer Provided Certificate

Call Home Customer Provided Certificate - Communication Path

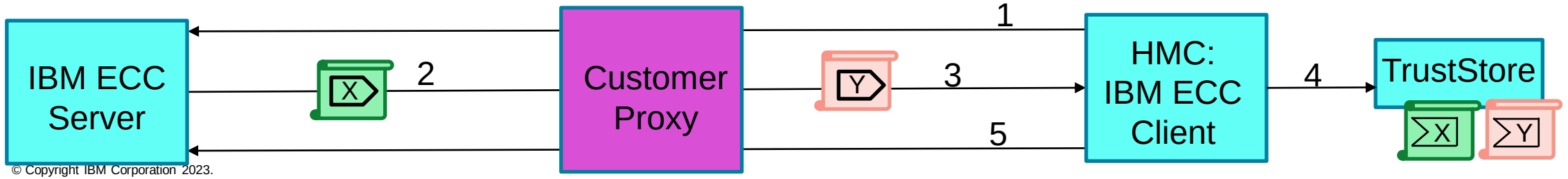
Call Home with no customer proxy Configured

1. Client initiates communication with the ECC Server.
2. The ECC Server presents certificate to client. (X)
3. Client has matching certificate (X) in TrustStore, so communication is allowed.
4. Communication continues with session certificates.



Call Home with customer proxy Configured

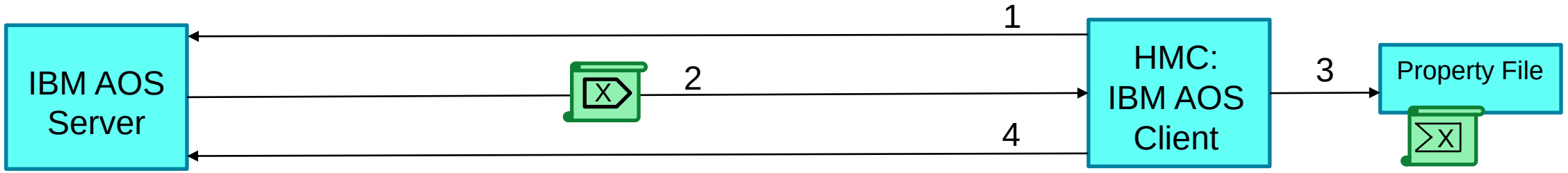
1. Client initiates communication with the ECC Server through the customer proxy server.
2. ECC Server presents certificate (X) to proxy.
3. Proxy presents Customer supplied certificate (Y) to client on HMC.
4. Client has matching certificate (Y) in the TrustStore, so proxy allows communication. Note that client still has original certificate (X) in the event Call home is not configured with Proxy.
5. Communication Continues with session certificates through the customer proxy.



AOS Customer Provided Certificate - Communication Path

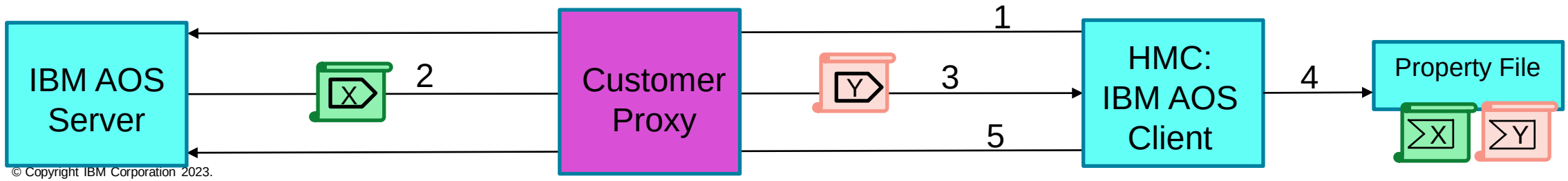
AOS with no customer proxy Configured

1. Client initiates communication with the AOS Server.
2. The AOS Server presents certificate to client. (X)
3. Client has matching certificate (X) in lightsoutprofile property file, so communication is allowed.
4. Communication continues with session certificates.



AOS with customer proxy Configured

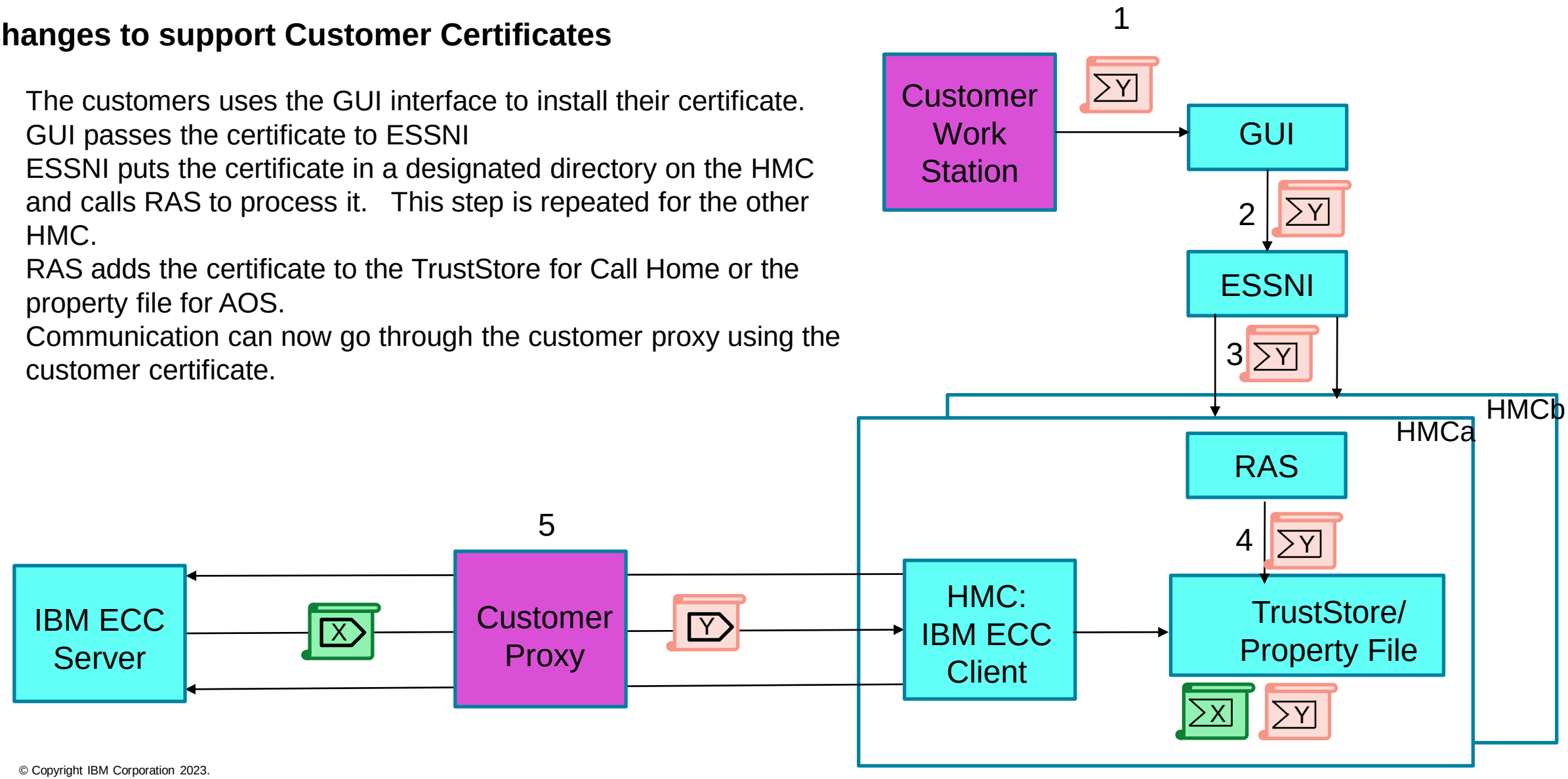
1. Client initiates communication with the AOS Server through the customer proxy server.
2. AOS Server presents certificate (X) to proxy.
3. Proxy presents Customer supplied certificate (Y) to client on HMC.
4. Client has matching certificate (Y) in the lightsoutprofile property file, so proxy allows communication. Note that client still has original certificate (X) in the property file, but it is not configured with Proxy.
5. Communication Continues with session certificates through the customer proxy.



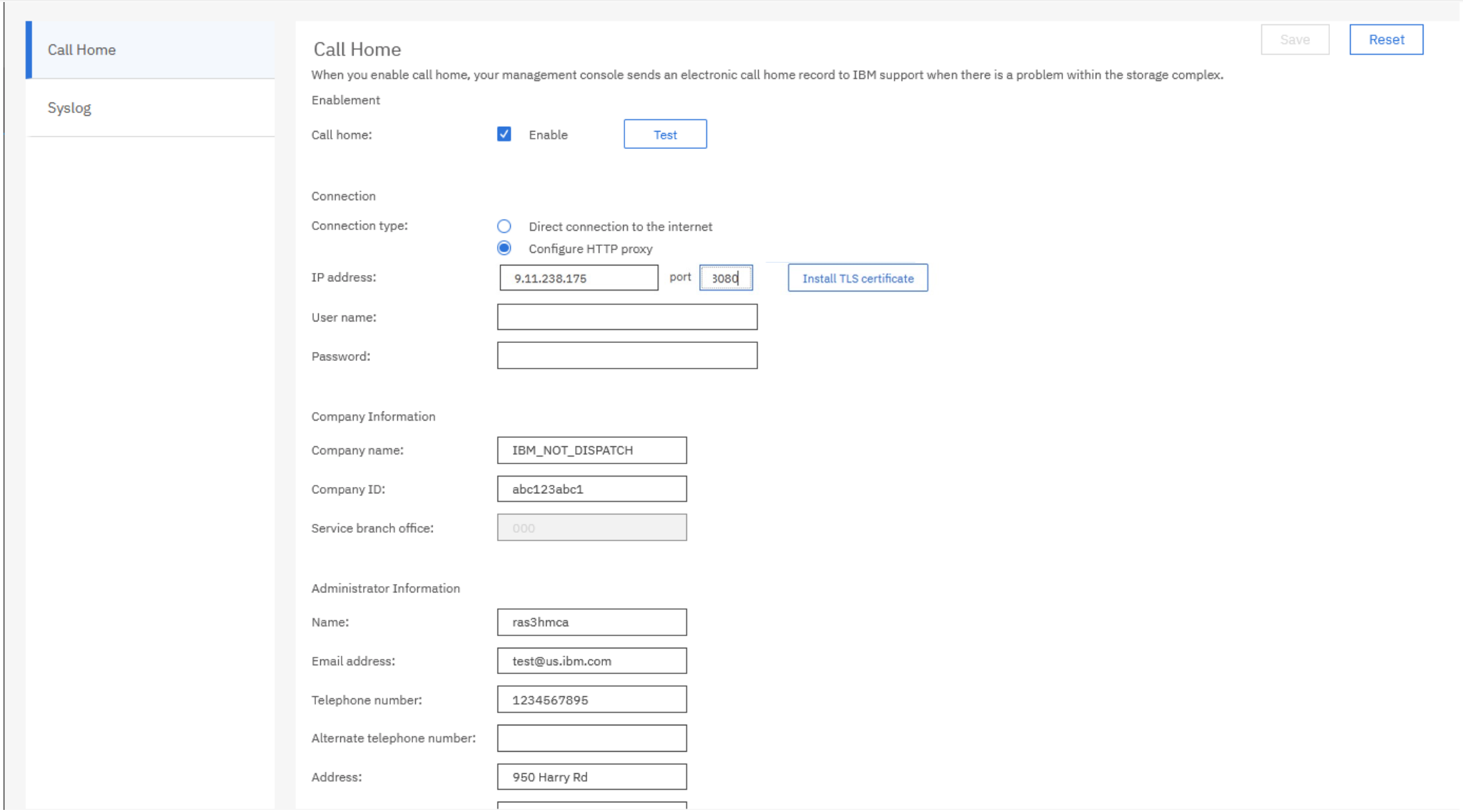
Call Home/AOS Customer Provided Certificate - New Support

Changes to support Customer Certificates

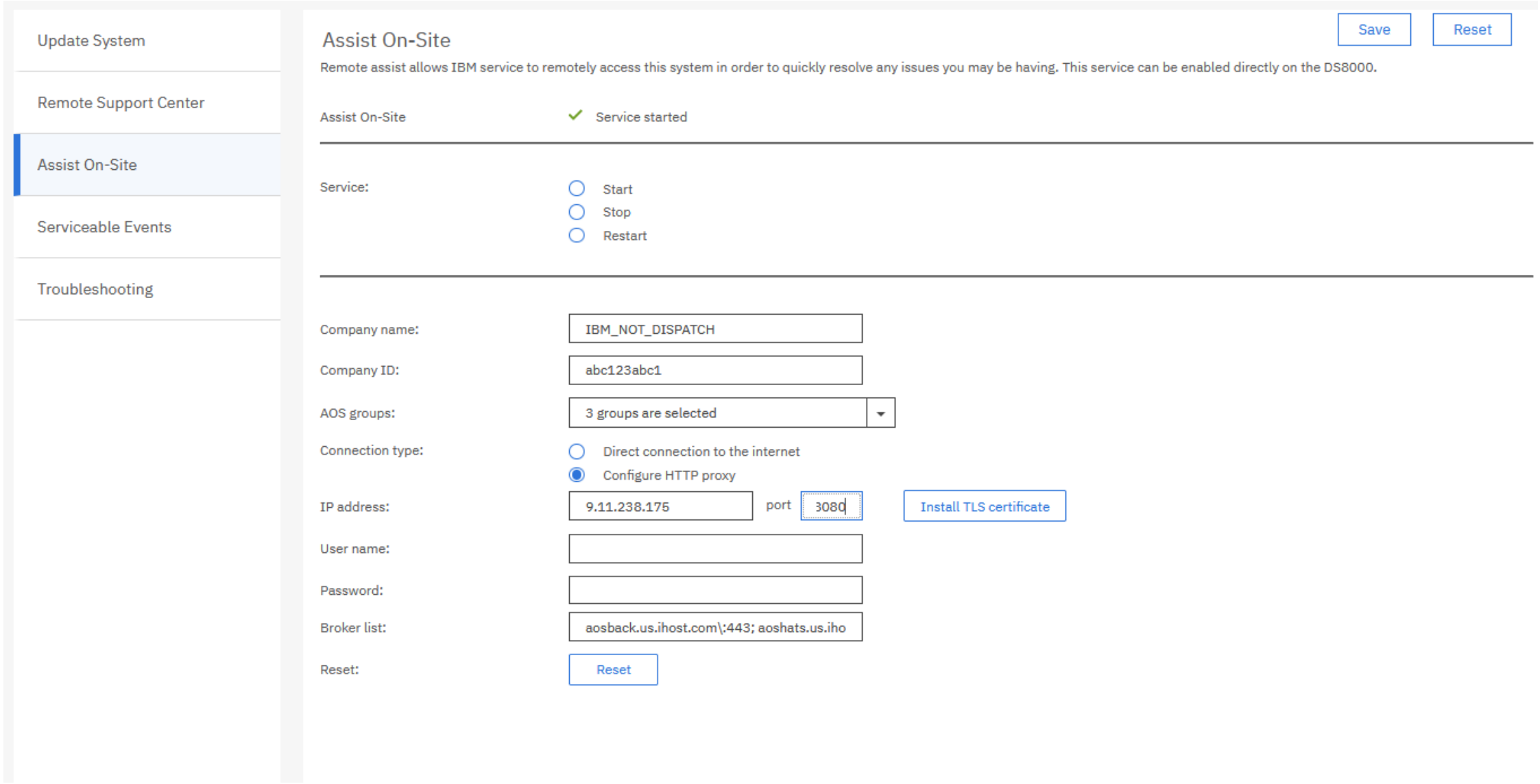
1. The customers uses the GUI interface to install their certificate.
2. GUI passes the certificate to ESSNI
3. ESSNI puts the certificate in a designated directory on the HMC and calls RAS to process it. This step is repeated for the other HMC.
4. RAS adds the certificate to the TrustStore for Call Home or the property file for AOS.
5. Communication can now go through the customer proxy using the customer certificate.



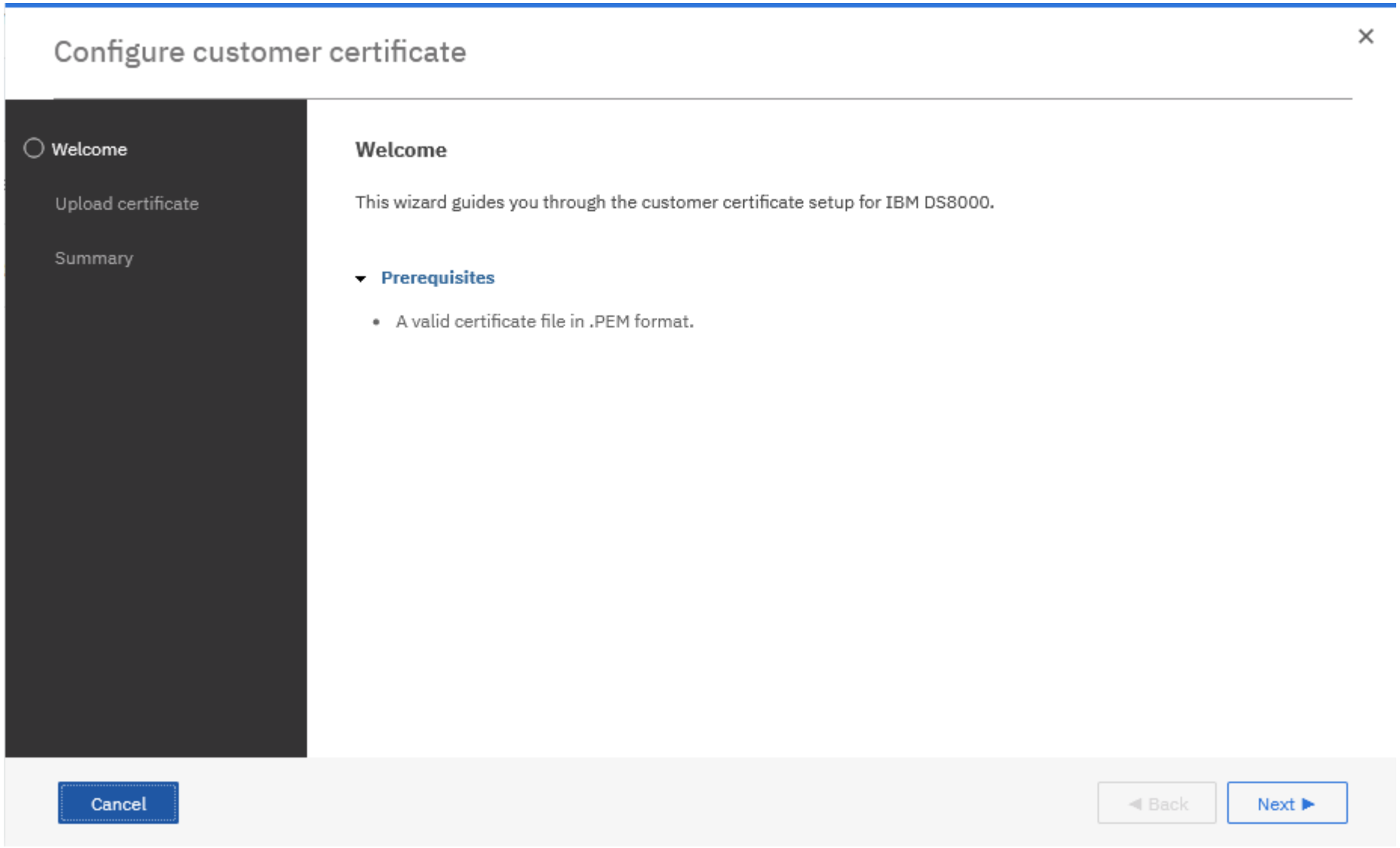
DS8950F GUI – Settings / Notifications



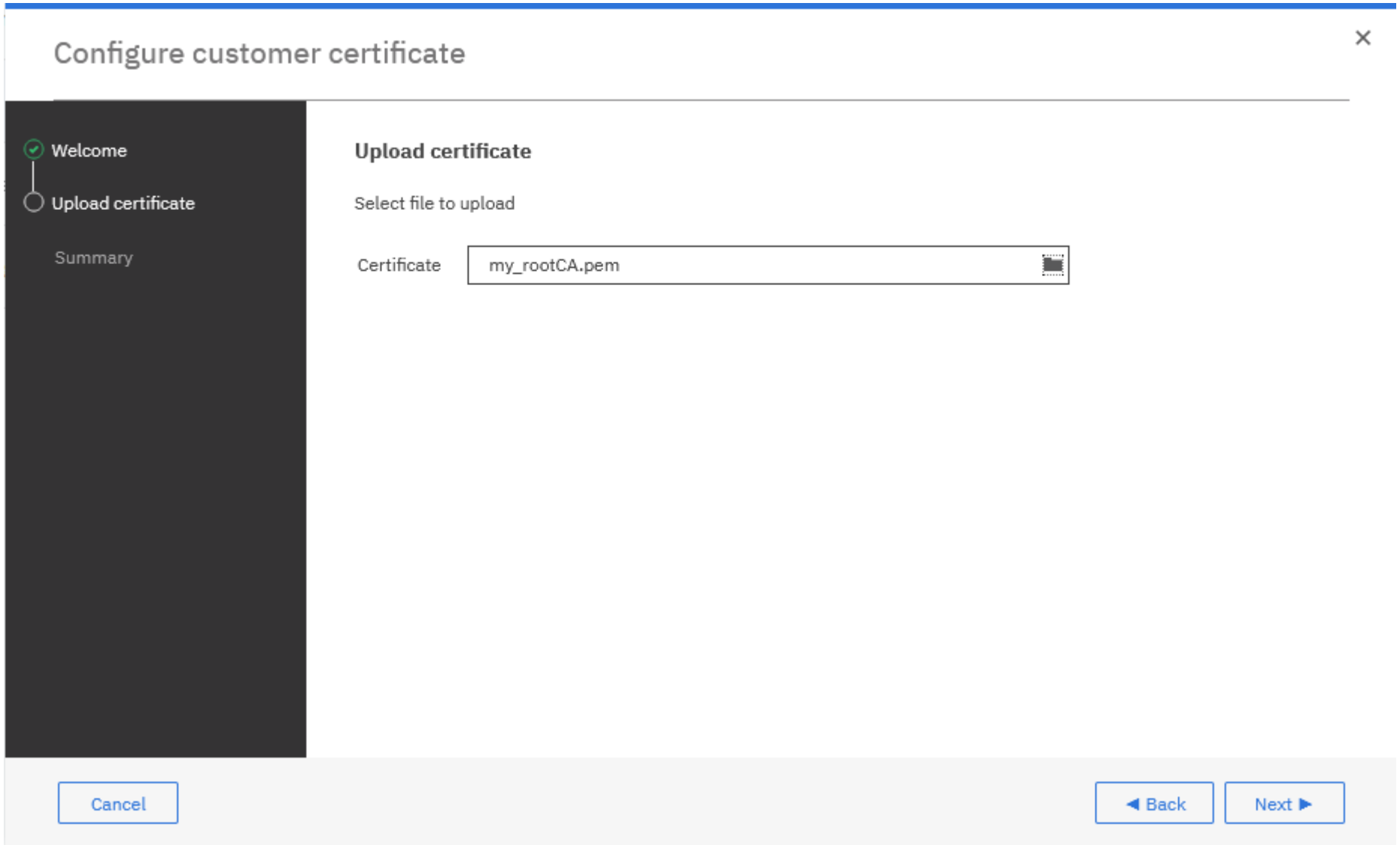
DS8950F GUI – Settings / Support / Assist On-Site



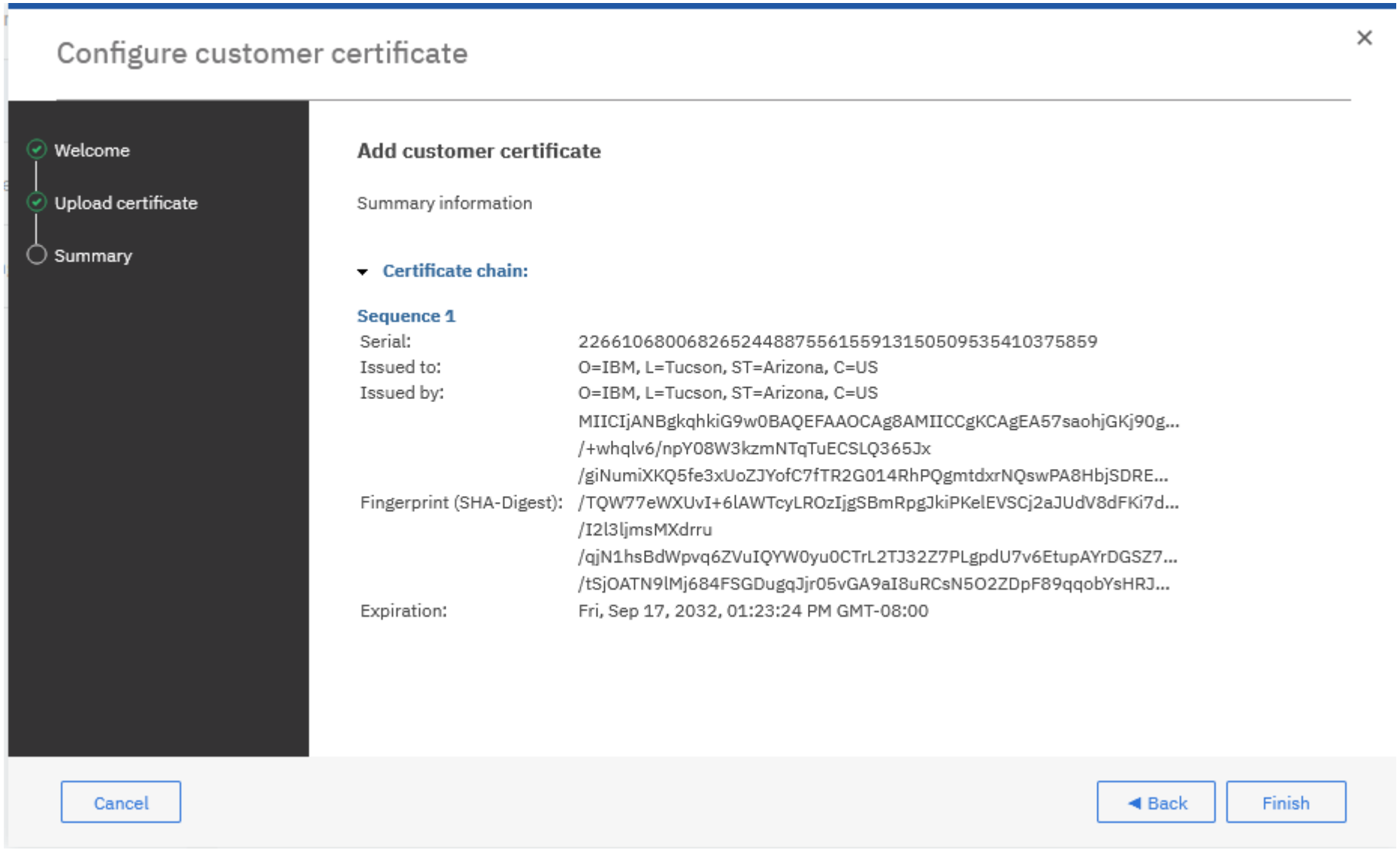
Install TLC Certificate Wizard (1 of 5)



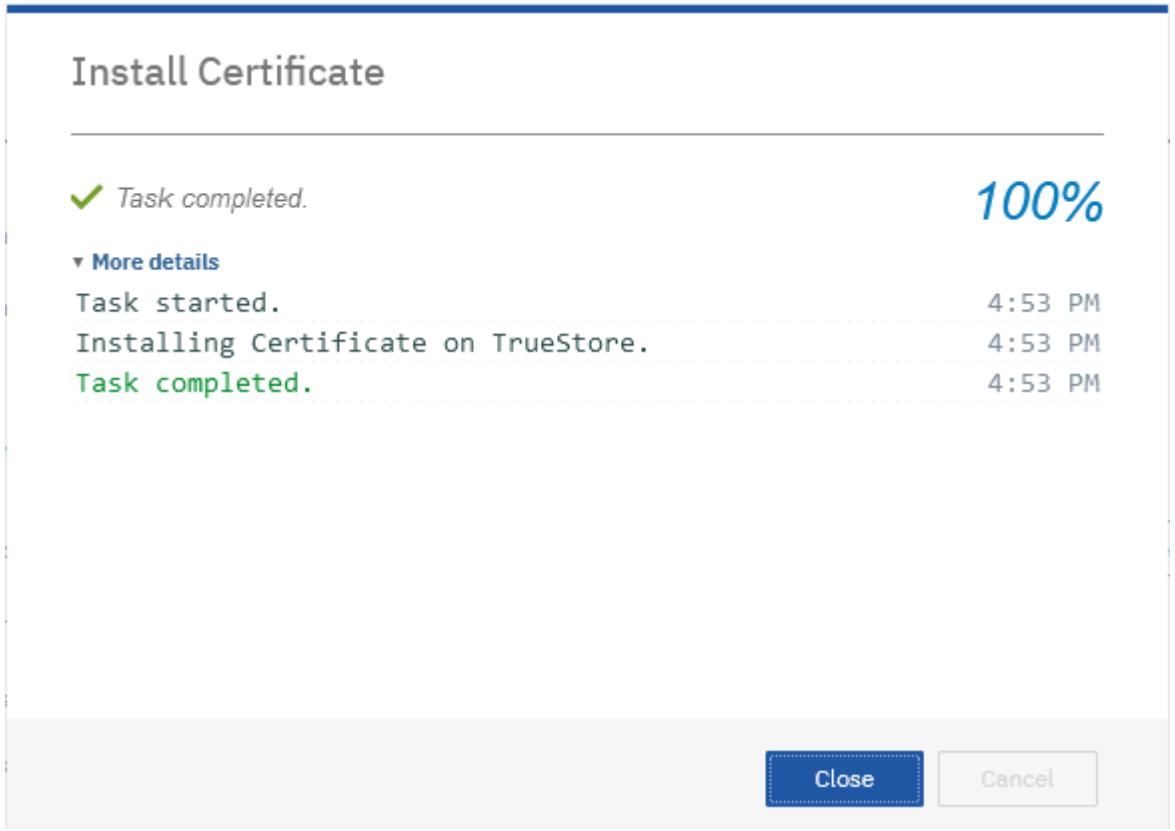
Install TLC Certificate Wizard (2 of 5)



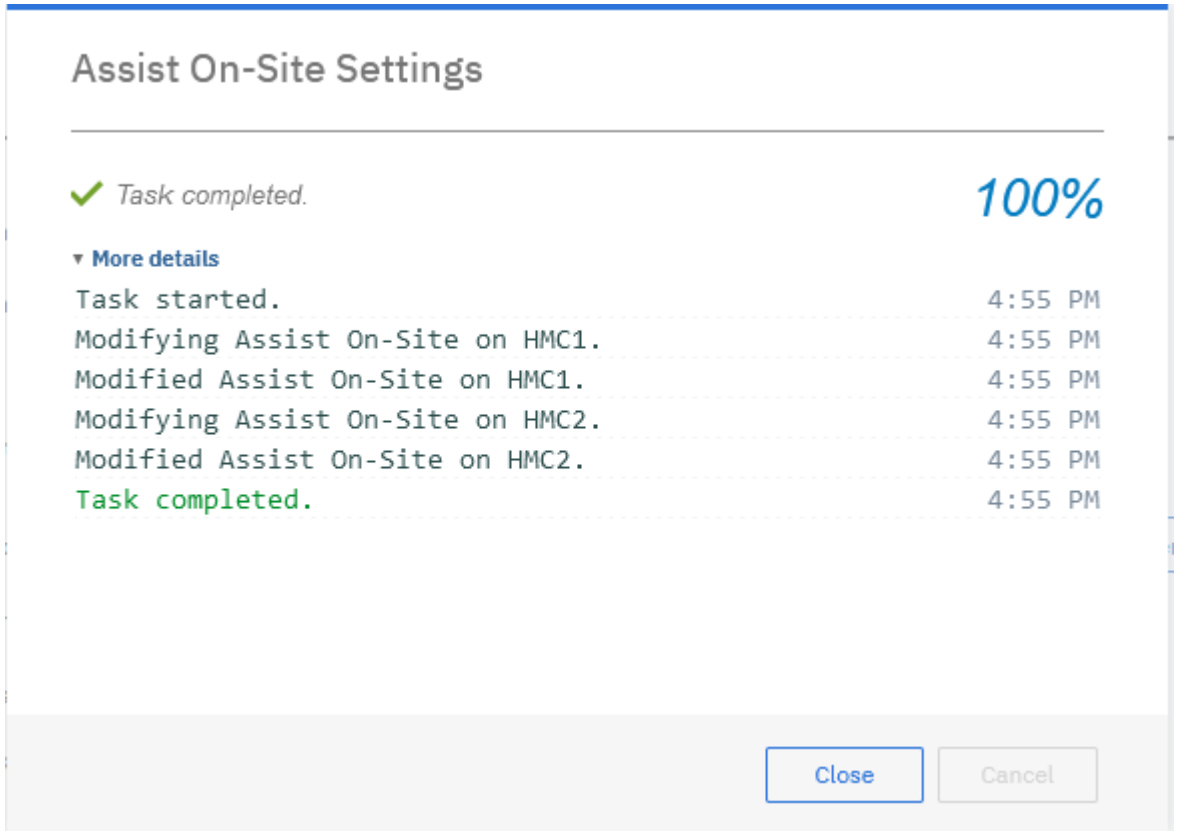
Install TLC Certificate Wizard (3 of 5)



Install TLC Certificate Wizard (4 of 5)



Install TLC Certificate Wizard (5 of 5)



Safeguarded Copy Enhancement

Safeguarded Copy Backup (SGC) Capacity - Background

- Two elements of Safeguarded Copy capacity
  - ✓Volume Capacity – defined on each volume in the SGC configuration (virtual capacity)
  - ✓Extent Pool Capacity – share capacity across all volumes in the pool (physical capacity)

- If a capacity threshold is met, the DS8900F will automatically expire the oldest SGC, in order to free up space to continue to capture changes
  - ✓When the oldest SGC is expired for the volume that exceeded the threshold, then subsequently the management software will detect this “roll-off” and will optionally expire all corresponding SGCs in the SGCset

- Volume Capacity threshold default is set at 98% of SGC volume capacity

- Extent Pool Capacity threshold default is set at 90% of extent pool capacity (prior to R9.3.2)

Challenges that need addressing

1. Exceeding available capacity

- ✓ Based on the configuration available, and the I/O workload that is being protected by Safeguarded Copy, reaching these thresholds may result in the customer having fewer SGC's than was planned
- ✓ Worst case: (most likely due to extent pool threshold) only a single SGC will remain, and possibly all available capacity could be consumed and volume(s) will be placed in a write inhibited mode

2. Mismatch of Global Mirror management threshold and SGC threshold

- ✓ There is an extent pool threshold for protecting Global Mirror consistency (default prior to R9.3.2 is 98%), so that if the target extent pool reaches the threshold, then Global Mirror will get suspended, protecting the last committed consistency group before the extent pool is completely exhausted
- ✓ In a Safeguarded Copy environment which is protecting the Global Mirror target volumes, the SGC extent pool threshold (default 90%, pre-R9.3.2) will be reached before the GM threshold, resulting in SGC backups being expired due to incoming write workload

Changes introduced in R9.3.2 (1 of 2)

- Introduce controls to define the minimum number of SGCs that must be preserved and not expired
- By default, this will be set to 1, and will result in similar behavior as in pre-R9.3.2
- Can be set in the range of 0 to 500
  - ✓ Setting to 0 will result in the SGC process being terminated (no more recording, no possible recovery from SGC) if only 1 SGC remains not expired, and space is exhausted
    - ➢ This protects production over SGCs – write inhibit will not be introduced, but the SGC process will terminate
  - ✓ Setting to 500 will not allow the internal rolloffs to occur, but you can still manage the retention period through management software
    - ➢ If capacity is exceeded, then automatic expiration is not possible and volumes will be placed in write inhibit state
- Behavior when either volume or extent pool capacity is above the threshold, and the minimum number of SGCs exist:
  - ✓ A new SGC request will fail during the reservation phase, with a new out of space sense code returned to the requestor
  - ✓ The current active SGC will continue to protect the environment, saving tracks that have already been captured but net new updates that continue to be received could push the capacity further past the threshold and to exhaustion

Changes introduced in R9.3.2 (2 of 2)

- Threshold changes:
  - ✓Global Mirror extent pool threshold reduced from 98% to 97%
  - ✓Safeguarded Copy extent pool threshold increased from 90% to 98%
  - ✓Safeguarded Copy volume level threshold remains at 98%
- Threshold changes will result in the Global Mirror process getting suspended, prior to the SGC thresholds being reached
- Specification of the minimum number of SGCs will be defaulted to 1 and can be changed to another value by opening a hardware support case against the DS8900F and requesting a change
  - ✓IBM would like to discuss the implications of the change in your environment, before activating this new behavior

Space Notifications

Safeguarded Copy & GDPS

So, why are we talking about Out of Space Messages, anyway?

Short answer: increased demand for Safeguarded Copy!

Adoption is driving clients to ask for GDPS enhancements to their SGC support. Several would like automated monitoring and reporting of SGC backup capacity. Others have requested function that would see GDPS automatically initiate a dynamic volume expansion for SGC back-up volumes.

These requests go hand-in-hand with an older RFE requesting that GDPS provide some sort of monitoring of space usage when it comes to space-efficient extent pools in environments with Global Mirror and Flash Copy.

Out of Space Messages – Background

- Became a requirement when DS8K implemented thin-provisioning
- Used to notify hosts and/or users that a volume or extent pool has reached a capacity threshold or has completely exhausted its capacity
- Also used to indicate when an out of space condition has been relieved
- Usually resolved either by issuing a release space command, or by adding more actual capacity

- For Safeguarded Copy backup volumes there were new messages implemented to indicate a specific backup/consistency group was “rolled-off” in order to make space for the next back-up

- Messages are delivered to System Z/CKD hosts by generating Attention status, which prompts the host to issue CCWs to read the waiting message
- Attention status is only provided to hosts that have devices “online” i.e., have at least one base device as part of a path group
- Because Safeguarded Copy targets are not host-addressable by design – i.e. will never be “online” - Out of Space messages for SGC target volumes are presented on the source volume’s LSS/LCU

Out of Space Message Generation

- Out of Space messages are generated in two different ways
  - ✓Extent-pool related messages are presented to every online host on every LSS/LCU on the box
  - ✓Backup volume messages are only presented to hosts that have a volume online in the source LSS/LCU

- Extent Pool Messages
  - ✓Extent Pool messages that are sent out to every host online to every LSS are good at notifying every potential stakeholder
  - ✓Are essentially over-presented with duplicate messages presented to hosts running to multiple LSSes
  - ✓Messages can still be missed in disaster recovery environments where a secondary control unit might have no production online

- LSS/Volume-Specific Messages
  - ✓Single LSS messages are more efficient by limiting delivery only to production systems online to that LSS
  - ✓Non-production management or disaster recovery systems like GDPS require explicitly configured paths and devices to each LSS they would like to receive Out of Space messages for
  - ✓No hosts online to a given LSS still leaves the chance that nobody will be notified of an out of space condition

New Message Generation Solution

- Allows a GDPS controlling system (K-sys) to receive *all* Out of Space messages generated by a managed DS8900F
- Minimizes the need for extra logical paths or volumes defined to the K-Sys
- Limits any extra message presentation to only systems that need to know
- Preserves existing DS8900F message presentation to avoid impacting existing customer configurations

- **Allow any interested hosts to explicitly register to receive Out of Space messages**

- Registered host systems will receive messages if they have at least one device online to that DS8900F cluster
- Easily applied in GDPS environments where utility devices are present on the managed DS8900Fs
- Easy to add two small utility devices and the associated paths to any DS8900F that doesn’t already have them defined
- Registered hosts will generally receive only one message per event, even if they have devices online to multiple LCUs

Co-requisites to exploit new function

Software Component	Required Level
SDM	zOS 2.4 or 2.5 with PTF UJ09789-HDZ2240 or UJ09790-HDZ2250
GDPS	GDPS 4.5 with APAR PH50146

Accelerate with ATG Technical Webinar Series - Survey

Please take a moment to share your feedback with our team!

You can access this 6-question survey via Menti.com with code 2243 3599 or

Direct link https://www.menti.com/albneqj15g57

Or

QR Code

Thank you!