User Administration (Amministrazione utente)

Virtual Desktop Service

NetApp
May 24, 2023

Sommario

User Administration (Amministrazione utente) . . . 1
Gestione degli account utente . . . 1
Gestione delle autorizzazioni per i dati . . . 3
Diritti dell’applicazione . . . 3
Reimposta password utente . . . 7
Autenticazione multifattore (MFA) . . . 10

User Administration (Amministrazione utente)

Gestione degli account utente

Crea nuovi utenti

Gli amministratori possono aggiungere utenti facendo clic su aree di lavoro > utenti e gruppi > Aggiungi/importa

Gli utenti possono essere aggiunti singolarmente o con un'importazione in blocco.

[larghezza=25%]

> L'accuratezza dell'e-mail e del numero di telefono cellulare in questa fase migliora notevolmente il processo di abilitazione dell'MFA in un secondo momento.

Una volta creati gli utenti, puoi fare clic sul loro nome per visualizzare dettagli come quando sono stati creati, il loro stato di connessione (sia che siano attualmente connessi o meno) e le relative impostazioni specifiche.

Attivazione di Virtual Desktop per gli utenti ad esistenti

Se gli utenti sono già presenti in ad, è possibile attivare il Virtual Desktop degli utenti facendo clic sull'ingranaggio accanto al nome e attivando il desktop.[larghezza=50%]

> Solo per Azure ad Domain Service: Affinché gli accessi funzionino, l'hash della password per gli utenti di Azure ad deve essere sincronizzato per supportare l'autenticazione NTLM e Kerberos. Il modo più semplice per eseguire questa operazione consiste nel modificare la password utente in Office.com o nel portale Azure, che forzerà la sincronizzazione dell'hash della password. Il ciclo di sincronizzazione per i server Domain Service può richiedere fino a 20 minuti, pertanto le modifiche alle password in Azure ad richiedono in genere 20 minuti per essere riflesse in AADDS e quindi nell'ambiente VDS.

Elimina account utente

Modificare le informazioni dell'utente

Nella pagina dei dettagli dell'utente è possibile modificare i dettagli dell'utente, ad esempio il nome utente e i dettagli di contatto. I valori di e-mail e telefono vengono utilizzati per il processo di reimpostazione self-service della password (SSPR).

[]

Modificare le impostazioni di sicurezza dell'utente

- VDI User Enabled (utente VDI abilitato) - impostazione RDS che, se attivata, crea un host di sessione VM dedicato e assegna a questo utente l'unico utente a cui si connette. Durante l'attivazione di questa casella di controllo, all'amministratore di CWMS viene richiesto di selezionare immagine, dimensione e tipo di storage della macchina virtuale.
  - Gli utenti AVD VDI devono essere gestiti nella pagina AVD come pool di host VDI.
- Scadenza account attivata: Consente all'amministratore di CWMS di impostare una data di scadenza

sull'account dell'utente finale.

- Imponi reimpostazione password al prossimo accesso: Richiede all'utente finale di modificare la password al successivo accesso.
- Multi-Factor Auth Enabled (autenticazione multifattore abilitata): Attiva l'autenticazione MFA per l'utente finale e richiede di configurare l'autenticazione MFA al successivo accesso.
- Mobile Drive Enabled (disco mobile abilitato): Una funzione legacy non utilizzata nelle implementazioni correnti di RDS o AVD.
- Local Drive Access Enabled (accesso al disco locale abilitato): Consente all'utente finale di accedere allo storage del dispositivo locale dall'ambiente cloud, tra cui Copy/Paste, USB Mass Storage e dischi di sistema.
- Wake on Demand Enabled (attiva su richiesta attivata): Per gli utenti RDS che si connettono tramite il client CW per Windows, l'abilitazione di questa opzione consente all'utente finale di portare il proprio ambiente quando si effettua la connessione al di fuori del normale orario di lavoro, come definito dalla pianificazione del carico di lavoro.

Account bloccato

Per impostazione predefinita, cinque tentativi di accesso non riusciti bloccano l'account utente. L'account utente si sbloccherà dopo 30 minuti, a meno che l'opzione *Enable Password complessità* non sia attivata. Se la complessità della password è attivata, l'account non viene sbloccato automaticamente. In entrambi i casi, l'amministratore VDS può sbloccare manualmente l'account utente dalla pagina utenti/gruppi in VDS.

Reimpostare la password dell'utente

Ripristina la password utente.

Nota: Quando si reimpostano le password degli utenti di Azure ad (o si sblocca un account), può verificarsi un ritardo fino a 20 minuti poiché la reimpostazione si propaga attraverso Azure ad.

Accesso amministratore

Abilitando questa opzione, l'utente finale ha accesso limitato al portale di gestione per il tenant. Gli usi più comuni includono la possibilità di fornire a un dipendente on-site l'accesso per reimpostare le password dei peer, assegnare l'applicazione o consentire l'accesso manuale all'attivazione del server. Vengono impostate anche le autorizzazioni che controllano le aree della console.

Disconnettersi dagli utenti

Gli utenti connessi possono essere disconnessi dall'amministratore VDS dalla pagina utenti/gruppi in VDS.

Applicazioni

Visualizza l'applicazione implementata in questo spazio di lavoro. La casella di controllo fornisce le applicazioni a questo utente specifico. La documentazione completa sulla gestione delle applicazioni è disponibile qui. L'accesso alle applicazioni può essere concesso anche dall'interfaccia App o ai gruppi di sicurezza.

Visualizzare/eliminare i processi degli utenti

Visualizza i processi attualmente in esecuzione nella sessione dell'utente. I processi possono essere terminati anche da questa interfaccia.

Gestione delle autorizzazioni per i dati

Prospettiva dell'utente finale

Gli utenti finali di Virtual Desktop possono accedere a diversi dischi mappati. Questi dischi includono una condivisione di team accessibile ai FTP, una condivisione file aziendale e il disco principale (per documenti, desktop, ecc.…) . Tutte queste unità mappate fanno riferimento a un livello di storage centrale su un servizio di storage (come Azure NetApp Files) o su una macchina virtuale del file server.

A seconda della configurazione di cui l'utente potrebbe non avere le unità H: O F: Esposte, potrebbero vedere solo il proprio desktop, documenti, ecc.… cartelle. Inoltre, l'amministratore del VDS può impostare lettere di unità diverse al momento dell'implementazione.[]

[]

Gestione delle autorizzazioni

VDS consente agli amministratori di modificare i gruppi di sicurezza e le autorizzazioni delle cartelle, tutto dal portale VDS.

Gruppi di sicurezza

I gruppi di sicurezza vengono gestiti facendo clic su Workspace > Nome tenant > utenti e gruppi > nella sezione gruppi

In questa sezione è possibile:

1. Creare nuovi gruppi di sicurezza
2. Aggiungere/rimuovere utenti ai gruppi
3. Assegnare le applicazioni ai gruppi
4. Attiva/disattiva l'accesso al disco locale ai gruppi

[]

Permessi della cartella

Per gestire le autorizzazioni delle cartelle, fare clic su Workspace > Nome tenant > Gestisci (nella sezione cartelle).

In questa sezione è possibile:

1. Aggiungi/Elimina cartelle
2. Assegnare autorizzazioni a utenti o gruppi
3. Personalizzare le autorizzazioni per sola lettura, controllo completo e Nessuna

[]

Diritti dell'applicazione

Panoramica

VDS dispone di un'efficace funzionalità integrata di autorizzazione e automazione delle applicazioni. Questa

funzionalità consente agli utenti di accedere a diverse applicazioni durante la connessione agli stessi host di sessione. Ciò è possibile grazie ad alcuni oggetti Criteri di gruppo personalizzati che nascondono i collegamenti insieme all'automazione che posiziona i collegamenti in modo selettivo sui desktop degli utenti.

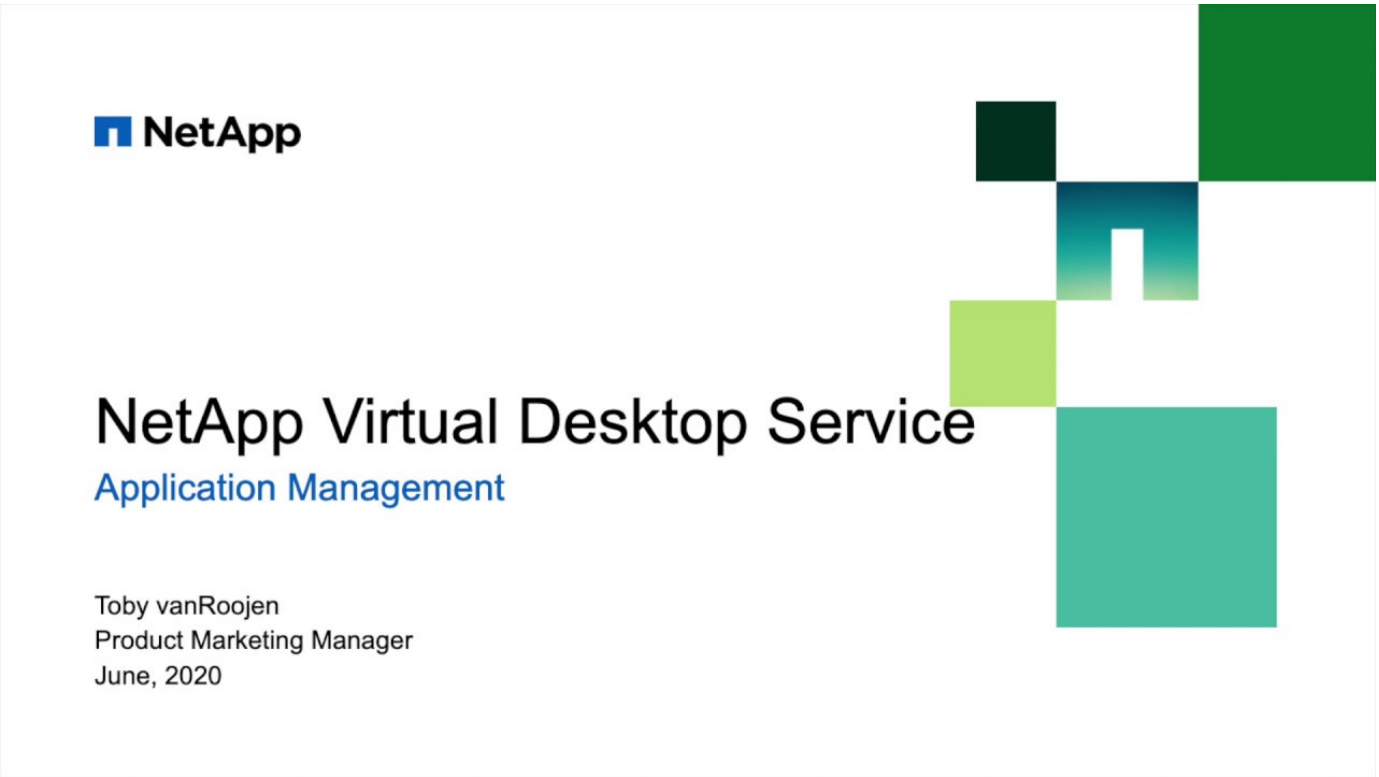
Questo flusso di lavoro si applica solo alle implementazioni RDS. Per la documentazione relativa ai diritti dell'applicazione AVD, vedere "Application Entitlement Workflow per AVD"

Le applicazioni possono essere assegnate agli utenti direttamente o tramite gruppi di sicurezza gestiti in VDS.

Ad alto livello, il processo di provisioning dell'applicazione segue questi passaggi.

1. Aggiungi app all'App Catalog
2. Aggiungi app all'area di lavoro
3. Installare l'applicazione su tutti gli host di sessione
4. Selezionare il percorso di scelta rapida
5. Assegnare le applicazioni a utenti e/o gruppi

I passaggi 3 e 4 possono essere completamente automatizzati con gli eventi con script, come illustrato di seguito



Video - Panoramica

Aggiungere applicazioni all'App Catalog

VDS Application Entitlement inizia con App Catalog, un elenco di tutte le applicazioni disponibili per l'implementazione negli ambienti degli utenti finali.

Per aggiungere applicazioni al catalogo, procedere come segue

1. Accedere a VDS all'indirizzo https://manage.cloudworkspace.com utilizzando le credenziali di

amministratore principali.

2. In alto a destra, fare clic sull'icona a forma di freccia accanto al nome utente e selezionare Impostazioni.
3. Fare clic sulla scheda App Catalog.
4. Fare clic sull'opzione Add App (Aggiungi applicazione) nella barra del titolo del catalogo applicazioni.
5. Per aggiungere un gruppo di applicazioni, selezionare l'opzione Importa applicazioni.
    a. Viene visualizzata una finestra di dialogo che fornisce un modello Excel da scaricare che crea il formato corretto per l'elenco delle applicazioni.
    b. Per questa valutazione, NetApp VDS ha creato un elenco di applicazioni di esempio per l'importazione, disponibile qui.
    c. Fare clic sull'area Upload (carica) e scegliere il file di modello dell'applicazione, quindi fare clic sul pulsante Import (Importa).
6. Per aggiungere singole applicazioni, selezionare il pulsante Add App (Aggiungi applicazione) per visualizzare una finestra di dialogo.
    a. Inserire il nome dell'applicazione.
    b. L'ID esterno può essere utilizzato per inserire un identificativo di tracciamento interno, ad esempio una SKU di prodotto o un codice di tracciamento della fatturazione (opzionale).
    c. Selezionare la casella di controllo Subscription (abbonamento) se si desidera creare un report sulle applicazioni come prodotto in abbonamento (opzionale).
    d. Se il prodotto non viene installato in base alla versione (ad esempio Chrome), selezionare la casella di controllo versione non richiesta. In questo modo è possibile installare i prodotti con aggiornamenti continui senza tenere traccia delle loro versioni.
    e. Al contrario, se un prodotto supporta più versioni con nome (ad esempio QuickBooks), selezionare questa casella per installare più versioni e avere VDS specifico per ciascuna versione disponibile nell'elenco delle applicazioni che possono avere diritto e per l'utente finale.
    f. Selezionare l'opzione "Nessuna icona di desktop utente" se non si desidera che VDS provi un'icona di desktop per questo prodotto. Viene utilizzato per prodotti "back-end" come SQL Server, poiché gli utenti finali non dispongono di un'applicazione a cui accedere.
    g. "L'app deve essere associata" impone la necessità di installare un'app associata. Ad esempio, un'applicazione client server potrebbe richiedere l'installazione di SQL Server o MySQL.
    h. Selezionando la casella licenza richiesta, VDS deve richiedere il caricamento di un file di licenza per un'installazione dell'applicazione prima di impostare lo stato dell'applicazione su attivo. Questa fase viene eseguita nella pagina Application Detail di VDS.
    i. Visibile a tutti: I diritti dell'applicazione possono essere limitati a specifici partner secondari in una gerarchia multicanale. A scopo di valutazione, fare clic sulla casella di controllo in modo che tutti gli utenti possano visualizzarla nell'elenco delle applicazioni disponibili.

Aggiungere l'applicazione all'area di lavoro

Per avviare il processo di implementazione, aggiungerai l'applicazione allo spazio di lavoro.

Per eseguire questa operazione, attenersi alla seguente procedura

1. Fare clic su aree di lavoro
2. Scorrere verso il basso fino ad applicazioni
3. Fare clic su Aggiungi
4. Selezionare le applicazioni, inserire le informazioni richieste, fare clic su Add Application (Aggiungi

applicazione), quindi su Add Apps (Aggiungi applicazioni).

Installare manualmente l’applicazione

Una volta aggiunta l’applicazione all’area di lavoro, è necessario installarla su tutti gli host di sessione. Questa operazione può essere eseguita manualmente e/o può essere automatizzata.

Per installare manualmente le applicazioni sugli host di sessione, attenersi alla seguente procedura

1. Accedere a Service Board (scheda di servizio).
2. Fare clic sull’attività del Service Board.
3. Fare clic sui nomi dei server per connettersi come amministratore locale.
4. Installare le applicazioni, verificare che il collegamento a questa applicazione si trovi nel percorso del menu Start.
    a. Per Server 2016 e Windows 10: C: ProgramData/Microsoft/Windows/Menu Start/programmi.
5. Tornare all’attività del Service Board, fare clic su Browse (Sfoglia) e scegliere il collegamento o una cartella contenente i collegamenti.
6. Qualsiasi opzione selezionata viene visualizzata sul desktop dell’utente finale quando viene assegnata l’applicazione.
7. Le cartelle sono eccezionali quando un’applicazione è in realtà costituita da più applicazioni. Ad esempio, "Microsoft Office" è più semplice da implementare come cartella con ogni applicazione come collegamento all’interno della cartella.
8. Fare clic su completa installazione.
9. Se necessario, aprire l’icona creata Add Service Board Task (Aggiungi attività Service Board) e confermare che l’icona è stata aggiunta.

Assegnare le applicazioni agli utenti

Il diritto all’applicazione viene gestito da VDS e l’applicazione può essere assegnata agli utenti in tre modi

Assegnare le applicazioni agli utenti

1. Accedere alla pagina User Detail (Dettagli utente).
2. Accedere alla sezione applicazioni.
3. Selezionare la casella accanto a tutte le applicazioni richieste dall’utente.

Assegnare gli utenti a un’applicazione

1. Accedere alla sezione applicazioni della pagina Dettagli area di lavoro.
2. Fare clic sul nome dell’applicazione.
3. Selezionare la casella accanto agli utenti dell’applicazione.

Assegnare applicazioni e utenti ai gruppi di utenti

1. Accedere ai dettagli di utenti e gruppi.
2. Aggiungere un nuovo gruppo o modificare un gruppo esistente.
3. Assegnare utenti e applicazioni al gruppo.

Reimposta password utente

Procedura di reimpostazione della password utente

1. Accedere alla pagina dei dettagli utilizzati in VDS

   []

2. Individuare la sezione Password, inserire due volte la nuova PW e fare clic su

   []

   []

È il momento di prendere effetto

- Per gli ambienti che eseguono un annuncio "interno" sulle macchine virtuali nell'ambiente, la modifica della password dovrebbe avere effetto immediato.
- Per gli ambienti che eseguono Azure ad Domain Services (AADDS), la modifica della password dovrebbe richiedere circa 20 minuti.
- Il tipo di ad può essere determinato nella pagina Deployment Details:

  []

Reimpostazione self-service della password (SSRP)

Il client NetApp VDS Windows e il client Web NetApp VDS forniscono una richiesta agli utenti che inseriscono una password errata quando accedono a un'implementazione di desktop virtuale v5.2 (o successiva). Nel caso in cui l'utente abbia bloccato l'account, questa procedura sbloccherà anche l'account dell'utente.

Nota: Gli utenti devono aver già inserito un numero di telefono cellulare o un indirizzo e-mail per poter eseguire questa procedura.

SSPR è supportato con:

- NetApp VDS Window Client
- Client Web NetApp VDS

In questa serie di istruzioni, verrà descritto il processo di utilizzo di SSPR come semplice mezzo per consentire agli utenti di reimpostare le password e sbloccare i propri account.

Client NetApp VDS Windows

1. In qualità di utente finale, fare clic sul collegamento Forgot Password (Password dimenticata) per continuare.

   []

2. Consente di selezionare se ricevere il codice tramite telefono cellulare o e-mail.

   []

3. Se un utente finale ha fornito solo uno di questi metodi di contatto, questo sarà l'unico metodo visualizzato.

   []

4. Al termine di questa fase, agli utenti viene visualizzato un campo Code (Codice) in cui inserire il valore numerico ricevuto sul dispositivo mobile o nella posta in arrivo (a seconda della selezione). Inserire il codice seguito dalla nuova password e fare clic su Reset (Ripristina) per continuare.

   []

5. Gli utenti visualizzeranno un messaggio che informa che la reimpostazione della password è stata completata correttamente. Fare clic su Done (fine) per completare il processo di accesso.

   > Se la distribuzione utilizza Azure Active Directory Domain Services, esiste un periodo di sincronizzazione delle password definito da Microsoft, ogni 20 minuti. Anche in questo caso, questo è controllato da Microsoft e non può essere modificato. Tenendo presente questo aspetto, VDS visualizza che l'utente deve attendere fino a 20 minuti per rendere effettiva la nuova password. Se la distribuzione non utilizza Azure Active Directory Domain Services, l'utente potrà effettuare nuovamente l'accesso in pochi secondi.

   []

Portale HTML5

1. Se l'utente non riesce a inserire la password corretta quando tenta di effettuare l'accesso tramite HTML5, viene visualizzata un'opzione per reimpostare la password:

   []

2. Dopo aver fatto clic sull'opzione per reimpostare la password, verranno visualizzate le opzioni di ripristino:

   []

3. Il pulsante 'Richiedi' invia un codice generato all'opzione selezionata (in questo caso l'email dell'utente). Il codice è valido per 15 minuti.

   []

4. La password è stata reimpostata. È importante ricordare che Windows Active Directory spesso richiede qualche istante per propagare la modifica, quindi se la nuova password non funziona immediatamente, attendere qualche minuto e riprovare. Ciò è particolarmente importante per gli utenti che risiedono in un'implementazione di servizi di dominio Active Directory di Azure, in cui la reimpostazione della password potrebbe richiedere fino a 20 minuti per la propagazione.

   []

Abilitazione della reimpostazione self-service della password (SSPR) per gli utenti

Per utilizzare la funzione di reimpostazione automatica della password (SSPR), gli amministratori devono prima inserire un numero di telefono cellulare e/o un account e-mail per un utente finale esistono due modi per inserire un numero di cellulare e gli indirizzi e-mail per un utente di desktop virtuale, come descritto di seguito.

In questa serie di istruzioni, verrà descritto il processo di configurazione di SSPR come un semplice mezzo per consentire agli utenti finali di reimpostare le password.

Importazione in blocco di utenti tramite VDS

Accedere al modulo Workspaces, quindi a Users & Groups e fare clic su Add/Import (Aggiungi/Importa).

È possibile inserire questi valori per gli utenti quando li creano uno alla volta:[]

In alternativa, è possibile includere questi elementi quando si importano in blocco utenti che scaricano e caricano il file XLSX Excel preconfigurato con questo contenuto completo:[]

Fornire i dati tramite l'API VDS

API NetApp VDS – in particolare questa chiamata https://api.cloudworkspace.com/5.4/swagger/ui/index#!/User/User_PutUser – consente di aggiornare queste informazioni.

Aggiornamento del telefono utente esistente

Aggiornare il numero di telefono dell'utente nella pagina User Detail Overview (Panoramica dettagli utente) di VDS.

[]

Utilizzo di altre console

Nota: Al momento non è possibile fornire un numero di telefono per un utente tramite Azure Console, Partner Center o dalla console di amministrazione di Office 365.

Personalizzare l'indirizzo di invio di SSPR

NetApp VDS può essere configurato per inviare l'email di conferma *from* a un indirizzo personalizzato. Si tratta di un servizio fornito ai partner dei provider di servizi che desiderano che i loro utenti finali ricevano l'e-mail di reimpostazione della password da inviare dal proprio dominio e-mail personalizzato.

Questa personalizzazione richiede alcuni passaggi aggiuntivi per verificare l'indirizzo di invio. Per avviare questo processo, aprire un caso di supporto con il supporto VDS richiedendo un "Self Service Password Reset Source Address" personalizzato. Definire quanto segue:

- Il tuo codice partner (puoi trovarlo facendo clic su *settings* sotto il menu con la freccia in alto a destra in basso). Vedere la schermata riportata di seguito)

  []

- Indirizzo "da" desiderato (che deve essere valido)
- A quali client applicare l'impostazione (o tutti)

Per aprire un caso di supporto, inviare un'e-mail all'indirizzo support@spotpc.netapp.com

Una volta ricevuto, il supporto VDS funzionerà per convalidare l'indirizzo con il nostro servizio SMTP e attivare questa impostazione. Idealmente, avrai la possibilità di aggiornare i record DNS pubblici nel dominio degli indirizzi di origine per massimizzare la deliverability della posta elettronica.

Complessità delle password

VDS può essere configurato per imporre la complessità delle password. L'impostazione per questa operazione si trova nella pagina dei dettagli dell'area di lavoro nella sezione Impostazioni dell'area di lavoro cloud.

[]

[]

Complessità della password: Disattivata

Policy	Linee guida
Lunghezza minima della password	8 caratteri
Validità massima password	110 giorni
Validità minima password	0 giorni
Imponi cronologia password	24 password memorizzate
Blocco password	Il blocco automatico si verifica dopo 5 immissioni errate
Durata blocco	30 minuti

Complessità della password: Attivata

Policy	Linee guida
Lunghezza minima della password	8 caratteri non contengono il nome dell'account dell'utente o parti del nome completo dell'utente che superano i due caratteri consecutivi contengono tre delle seguenti quattro categorie: Caratteri maiuscoli inglesi (Dalla A alla Z) caratteri minuscoli inglesi (dalla a alla z) 10 cifre di base (da 0 a 9) caratteri non alfabetici (ad esempio, !, €, n., %) i requisiti di complessità vengono applicati quando le password vengono modificate o create.
Validità massima password	110 giorni
Validità minima password	0 giorni
Imponi cronologia password	24 password memorizzate
Blocco password	Il blocco automatico si verifica dopo 5 immissioni errate
Durata blocco	Rimane bloccato fino a quando l'amministratore non si sblocca

Autenticazione multifattore (MFA)

Panoramica

NetApp Virtual Desktop Service (VDS) include un servizio MFA basato su SMS/e-mail senza costi aggiuntivi. Questo servizio è indipendente da qualsiasi altro servizio (ad esempio Azure Conditional Access) e può essere utilizzato per proteggere gli accessi degli amministratori a VDS e gli accessi degli utenti ai desktop virtuali.

Nozioni di base su MFA

- VDS MFA può essere assegnato a utenti admin, singoli utenti finali o applicato a tutti gli utenti finali
- VDS MFA può inviare notifiche via SMS o e-mail
- VDS MFA dispone di una funzione di configurazione e ripristino iniziali self-service

Scopo della guida

Questa guida illustra la configurazione di MFA insieme a un'illustrazione dell'esperienza dell'utente finale

Questa guida tratta i seguenti argomenti:

1. Abilitazione di MFA per singoli utenti
2. Richiede MFA per tutti gli utenti
3. Abilitazione di MFA per singoli amministratori
4. Configurazione iniziale dell'utente finale

Abilitazione di MFA per singoli utenti

L'autenticazione MFA può essere attivata per singoli utenti nella pagina dei dettagli dell'utente facendo clic su *Multi-Factor Auth Enabled*

Aree di lavoro > Nome area di lavoro > utenti e gruppi > Nome utente > autenticazione a più fattori attivata > Aggiorna

L'MFA può anche essere assegnato a tutti gli utenti; se questa impostazione è attiva, la casella di controllo viene selezionata e *(via Client Settings)* viene aggiunto all'etichetta della casella di controllo.

Richiede MFA per tutti gli utenti

L'MFA può essere attivato e applicato a tutti gli utenti nella pagina dei dettagli dell'area di lavoro facendo clic su *MFA for All Users Enabled*

Aree di lavoro > Nome area di lavoro > MFA per tutti gli utenti attivato > Aggiorna

Abilitazione di MFA per singoli amministratori

MFA è disponibile anche per gli account amministratore che accedono al portale VDS. Questa opzione può essere attivata per amministratore nella pagina dei dettagli dell'amministratore. Amministratori > Nome amministratore > autenticazione multifattore richiesta > Aggiorna

Configurazione iniziale

Al primo accesso dopo aver attivato MFA, all'utente o all'amministratore verrà richiesto di inserire un indirizzo e-mail o un numero di telefono cellulare. Riceveranno un codice di conferma per partecipare e confermare l'avvenuta registrazione.