



BeyondTrust

Privileged Access Discovery Application User Guide

Table of Contents

Privileged Access Discovery Application User Guide	3
Discovery Application Operating System Requirements	3
Supported Target Systems	4
Download and Setup	4
Preparatory Steps	5
Start Discovery Application	5
Targets	6
Delete Target	6
Credentials	7
Edit Credential	8
Delete Credential	8
Scan and Results	9
Discovery Report	10
Configure Windows Hosts for Discovery Scans	12

Privileged Access Discovery Application User Guide

The first step in addressing security risks related to privileged activity such as potential credential compromise or malicious activity from inside or outside of your organization (insiders and third parties), is an assessment of the privileged accounts on your network.

The free **Privileged Access Discovery Application (Discovery Application)** is an application that provides key information on the scope of privileged accounts, to equip you with the information you need to proactively protect them. The application scans server *targets*, and produces a customized report on findings. You get free, unlimited use, so run the application periodically or whenever your network changes.

This report is designed to give you a high-level overview of privileged activity information about the systems scanned on your network, including:

- Privileged accounts
- Password age
- SSH keys
- Services running with user accounts
- User accounts with administrative rights
- Remote access tools installed on your system

This guide provides instructions to set up and use the **Discovery Application**.

Discovery Application Operating System Requirements

Discovery Application can be run from any of these **64-bit** operating systems:

- Windows Vista
- Windows 7
- Windows 8
- Windows 10
- Server 2012
- Server 2016
- Server 2019



You also need .NET Framework (version 4.5.2 minimum, version 4.7 is recommended) installed for the scanner to operate properly.

Supported Target Systems

Discovery Application can scan any of these platforms:

Windows Workstations

- Windows Vista
- Windows 7
- Windows 8
- Windows 10

Windows Server

- Server 2012
- Server 2016
- Server 2019

Unix

- AIX
- Cisco
- HP iLO
- HP-UX
- Juniper
- Linux
- Mac OSX
- Palo Alto Networks
- Solaris
- vSphere SSH

Download and Setup

From the BeyondTrust website, download the **PrivilegedAccessDiscovery.zip** file. We suggest placing the file in an appropriate location before extracting its content.

To set up **Discovery Application**, right-click the **PrivilegedAccessDiscovery.zip** file, and then select **Extract All....**



Note: The application can only be run from Windows. It runs as a standalone, self-contained application.

Preparatory Steps

Prior to starting up and working with **Discovery Application**, we recommend that you:

- Ensure you have the correct credentials to allow you to perform the scan (you may need multiple credentials). You must use *admin* or *root* credentials for **Discovery Application**.
- Collect the *host names* or *IP addresses* of the targets you that you want to scan.



Tip: If you have a lot of systems you want to scan, we suggest you break them up into groups of scans, to keep your scan reports more manageable. For more information on how to format the target list, please see "[Targets](#)" on page 6.

Start Discovery Application

To start using **Discovery Application**:

1. Go to the folder where you have extracted the files, and then double-click the **Privileged Access Discovery.exe** file.
2. Read the License Agreement, and then check the box to accept the terms of the agreement.
3. (Optional). To download a printable copy of the license agreement, click the **Download License Agreement PDF** link.
4. Click **Accept**.

Get started with Privileged Access Discovery

With Privileged Access Discovery you can securely reveal unknown privileged accounts and credentials in your environment and much more. To get started we'll need you to accept the terms in the license agreement below.

License Agreement

 [Download License Agreement](#)

SOFTWARE LICENSE AND SERVICE AGREEMENT

IMPORTANT – PLEASE REVIEW CAREFULLY THE FOLLOWING TERMS AND CONDITIONS OF THIS PRIVILEGED ACCESS DISCOVERY END USER LICENSE AGREEMENT ("EULA"). THIS EULA IS ENTERED INTO BETWEEN BEYONDTTRUST AND LICENSEE AS OF THE EFFECTIVE DATE. LICENSEE HEREBY ENTERS INTO AND ACCEPTS THIS EULA AND THE TERMS AND CONDITIONS HEREOF. LICENSEE REPRESENTS THAT HE OR SHE IS AT LEAST 18 YEARS OF AGE.

In consideration of the mutual covenants contained herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties hereby agree as follows:

1. Definitions. Except as may otherwise be defined herein, the following terms are defined for the purposes of this EULA and any Order Form as follows:

☒ I accept the terms and do not wish to see this again the next time I run this version.

Accept

Privileged Access Discovery Version 22.1.0.501 Copyright 2022, BeyondTrust Corporation.

This computer program is protected by the copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe criminal penalties and will be prosecuted to the maximum extent of the law.

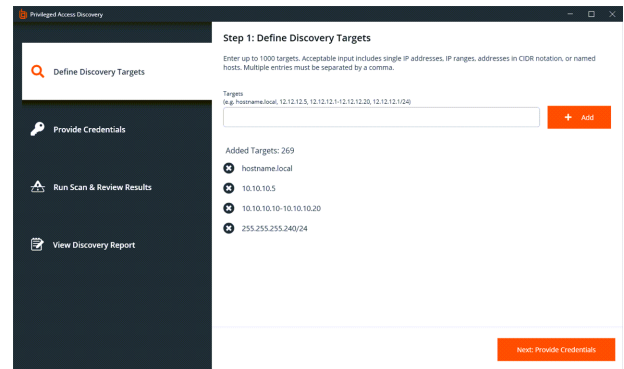
Targets

The **Targets** page is where you set the targets for the Discovery Scan. **Discovery Application** scans up to 1000 targets per scan.

Targets can be entered in the following formats:

- host name (example: **hostname.local**)
- single IP address (example: **10.10.10.5**)
- IP address range (example: **10.10.10.10-10.10.10.20**)
- IP address range in Classless Inter-Domain Routing (CIDR) format (example: **255.255.255.240/24**)

Enter a list of targets by separating the targets with a *comma* or *space*, as below.



Example: *hostname.local, 10.10.10.5, 10.10.10.10-10.10.10.20, 255.255.255.240/24.*

Once you click **+ Add**, they appear as separate entries in the list.



Tip: *If you have a large number of targets you want to scan, separate them into groups, run the scans and generate reports per group, to keep your scan reports manageable.*

Once you are finished entering targets, click **Next: Provide Credentials**.



Note: *Target information is only stored while you use the application. Once the scan is completed and the final report is generated, or when you click **Start Again** or close the application, all target information is deleted.*

Delete Target

To delete a target, at the left of a listed target, click the **X** to remove it from the current list.

Once you are finished entering targets, click **Next: Provide Credentials**.

Credentials

You can set up multiple credentials of the *Windows* or *SSH* credential type, to use for the Discovery Scan. Multiple credentials can facilitate scanning an environment where one set of credentials does not have privileges to all systems. For example, you might have one set of credentials for Windows and a different set for Linux systems. The application would use the credentials with the most privileges on each of the targets being scanned.



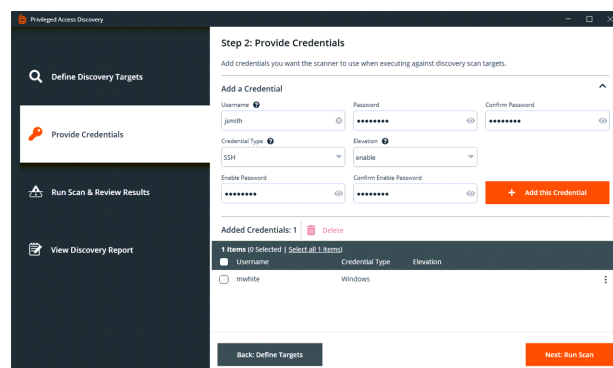
Note: Credential information is only stored while you use the application. Once the scan is completed and the final report is generated, or when you click **Start Again** or close the application, all credential information is deleted.



Note: When entering domain credentials, the following syntax must be used: **domain/username**.

To set credentials:

1. From the dropdown list, select the **Credential Type**. If you select the **SSH** type, an additional **Elevation** field appears below the password fields.
2. For **Windows** type credential:
 - Enter a **username**.
 - Enter the **password** for this username, then confirm the password.
 - Go to Step 4.
3. If you select the **SSH** credential type, elevating the credentials is optional. The default is **none**. If you select this option, enter a **username**, enter the **password** for this username, and then confirm the password. Go to Step 4.



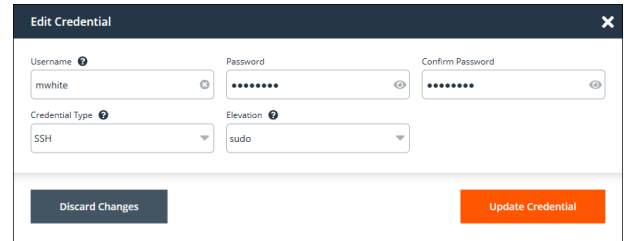
To choose a different option, from the **Elevation** dropdown list, select an option. Elevating the credentials provides more thorough scans.

- For **sudo**, in most cases, the optional sudo username would be blank. When blank, commands run with the effective privileges of the *root* account. If an optional username is entered, sudo runs in the security context of that user. Enter the **password** for this username, and then confirm the password. Go to Step 4.
 - For **pbrun**, enter the **pbrunuser** username. Enter the **password** for this username, and then confirm the password. Go to Step 4.
 - If you select the **enable** option, two additional password-related fields appear. Enter a **password** for Cisco devices, and then confirm the password. Go to Step 4.
4. Click **Add this Credential**. The credential appears in the list below.
 5. You can add as many credentials as you need to run scans. To enter additional credentials, start the process over again.
 6. Once you are finished entering credentials, click **Next: Run Scan**.

Edit Credential

To **edit** credentials in the list:

1. At the right of a credential listed, click the **ellipsis** icon, and then select **Edit Credential**.
2. In the **Edit Credential** dialog box, make the necessary changes, and then click **Update Credential**.
3. Click **Continue**.
4. Once you are finished entering credentials, click **Next: Run Scan**.



Delete Credential

To **delete** credentials from the list:

1. Check the box at the left of one or more credentials, and then click **Delete**.
2. Click **Confirm**.
3. Once you are finished entering credentials, click **Next: Run Scan**.

Scan and Results

The **Run Scan & Review Results** page displays the number of targets scanned, and when the scan process is complete.

Discovery Application uses the following short list of ports in every scan, regardless of what scan template is selected:

- **Standard Ports:** 22, 80, 110, 139, 389, 443, 445, 3389
- **Remote Access Ports** (besides 3389): 5631, 5632, 5901, 6129

To view the **Scan Log**, while the scan is in progress or when it's complete, click the **View Scan Log** button. The **Scan Log** window appears.

The **Scan Log** contains diagnostic level information which you can use to track the progress of the scan, and potentially identify failures for specific targets.

To close the window and get back to the **Run Scan & Review Results** page, click the **X** at the top right of the **Scan Log** window.

To run the scan again, click **Run Scan Again**.

The scan summary displays the following:

- The number of targets found and *successfully* authenticated.
- The number of targets found that *failed* authentication, including those *not found*.

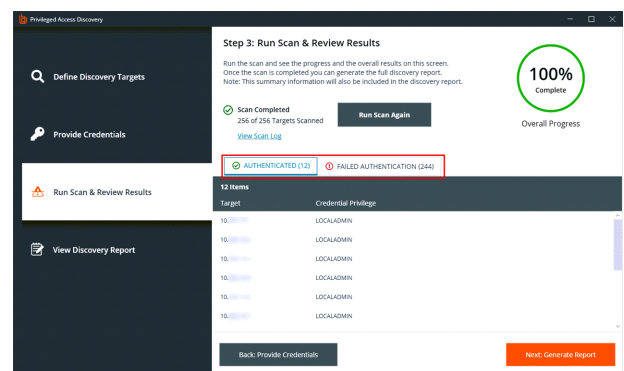
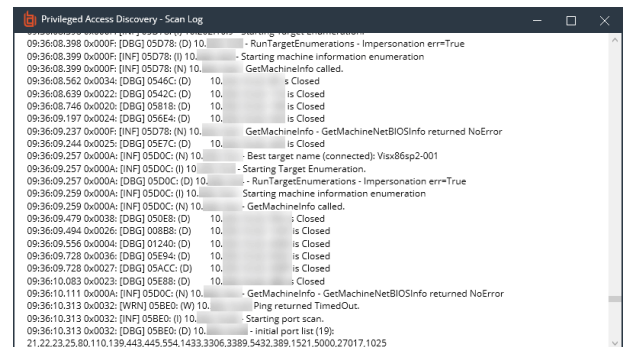
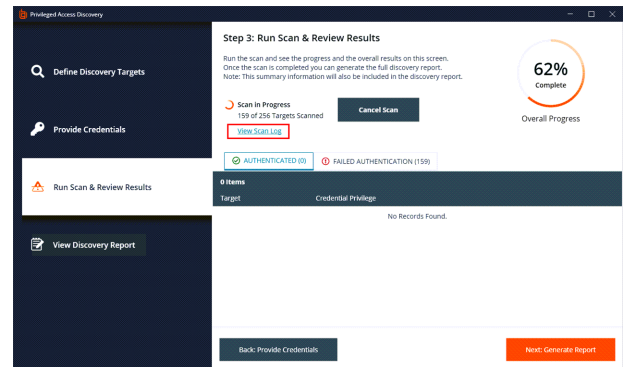
The default list view is of the successfully **Authenticated** targets.

- To view the list of targets that failed authentication, click the **Failed Authentication** heading.



Note: If you suspect that a target should have been found and was not, then please ensure that the target is routable from the machine you have installed the **Discovery Application**.

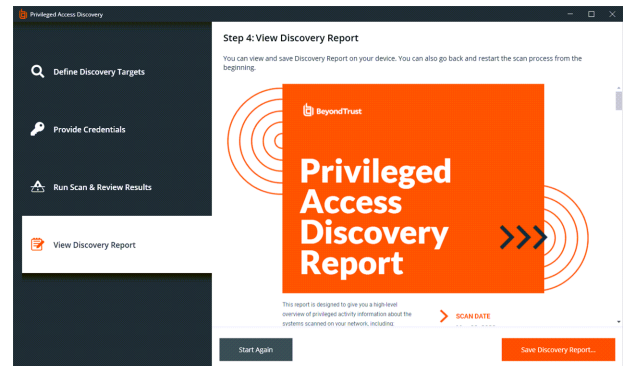
- To generate a report and move to the **Discovery Report** page, click **Next: Generate Report**.



Discovery Report

The data in this report is available for your organization to use in the effort of protecting your infrastructure from cyber threats. While the report displays onscreen within **Discovery Application**, you can also download a copy as a .PDF or an .XLSX file.

The **View Discovery Report** page displays the PDF format report, which you can scroll through to view the results.



To save a PDF copy of the report, click **Save Discovery Report...**, and then select **Save Report (.pdf)**.



You can also save the report as a *spreadsheet* (.xlsx) file, which provides you with more detailed information such as *details of the scanned targets, discovered user accounts, services, software*, and more. Save a spreadsheet report and explore the information categories provided.

	A	B	C	D	E	F	G	H	I	J	K	L	M
223	89C5DD0B-E4BD-435E-9B32-40CDD6481316		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
224	E432D490-FD54-4FC0-8665-93970658702		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
225	D0D94D69-20BF-4154-9939-77017AB14A6F		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
226	EC839D25-0FA0-4A08-ABEA-8890D64BC6F3		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
227	189B9C62-2892-4430-8FFE-667061879421		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
228	469A18C1-4DEB-415F-9C5F-6D05A48EA8AC		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
229	83C9CBF8-0005-4422-9121-AC0715AD4292		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
230	BCA6CFE2-5D06-4DC3-82B5-E4822258A3C		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
231	78676F90-835B-4C35-86B8-494891058332		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
232	8B324CA7-3282-4956-BD83-417A19532248		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
233	E36D319A-7BF2-4EB1-95A9-BA9AA6C6CA42		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
234	6154F780-46B5-4826-8C50-75B21276E015		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
235	5E5FD01A-7F0D-457F-9175-EA695D87C06C		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
236	BE7E82C3-AEA3-4992-A14B-A7E5E5C0FF76		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
237	D5E7EC74-2574-492E-912F-9A13C5839214		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
238	1939633A-D9B6-462F-AD6C-36A68080E6F2		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
239	8BCBA393-8E7D-4336-B907-8B7C0F02C896		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
240	780515D6-4996-4D72-94DF-434D74882828		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
241	D902753D-93C4-4F4C-95A6-01F2F68BC180		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
242	9D7B38AD-9F8C-4AEC-918E-80594328B481		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
243	06019DCC-9D2E-4E54-A0E5-03F87DE368CD		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
244	1D1FF52A-CD3A-413C-B8D2-397D0D3A3580		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
245	317FCA72-9E23-4FBA-99CC-B0CF12E8D818		Unknown OS				10.			GUEST	FALSE	FALSE	No open port
246	7FA53B4B-A63D-4D06-A312-578C49E4D07D	VI	Windows Vista (TM) Enterprise	WORKGROUP	VISX86SP2-ESA	10.	2cc38280-a889-4d56-a7ec-56a2aa administrator	LOCALADMIN	FALSE	TRUE	Windows		
247	E88DE760-5D63-4812-A39B-360361C0A5A1	VI	Windows Vista (TM) Ultimate	WORKGROUP	VISX86SP2-001	10.	2cc38280-a889-4d56-a7ec-56a2aa administrator	LOCALADMIN	FALSE	TRUE	Windows		
248	8082ED3C-8B24-45E9-A8A9-CC774EF66676	VI	Windows Vista (TM) Enterprise			10.	2cc38280-a889-4d56-a7ec-56a2aa administrator	LOCALADMIN	FALSE	TRUE	Windows		
249	7D1E1A0B-0BA7-4994-866C-2167D4A50E7E	1C	Windows			10.	2cc38280-a889-4d56-a7ec-56a2aa administrator	LOCALADMIN	FALSE	TRUE	Windows		
250	F1454332-4A36-4C6A-9C5F-76B0913D965	VI	Windows Vista (TM) Ultimate	WORKGROUP	VISX64SP2-001	10.	2cc38280-a889-4d56-a7ec-56a2aa administrator	LOCALADMIN	FALSE	TRUE	Windows		
251	775A8D08-4F8B-4B74-8E5B-5081BDCDEFB7	1C	Windows			10.	2cc38280-a889-4d56-a7ec-56a2aa administrator	LOCALADMIN	FALSE	TRUE	Windows		
252	F8C27F90-6260-4337-970E-D77F08020082	1C	Windows			10.	2cc38280-a889-4d56-a7ec-56a2aa administrator	LOCALADMIN	FALSE	TRUE	Windows		
253	C19E2707-E626-43F1-955D-7923742326E2	2N	Windows Server 2008 R2 Enterprise			10.	2cc38280-a889-4d56-a7ec-56a2aa administrator	LOCALADMIN	FALSE	TRUE	Windows		
254	BE437039-E51A-4E67-A655-6BD8664169AF	1C	Windows Vista (TM) Ultimate			10.	2cc38280-a889-4d56-a7ec-56a2aa administrator	LOCALADMIN	FALSE	TRUE	Windows		
255	6D5D2A50-98AB-4DA1-8EA9-98ECC7A4411B	2N	Windows Server 2008 R2 Enterprise			10.	2cc38280-a889-4d56-a7ec-56a2aa administrator	LOCALADMIN	FALSE	TRUE	Windows		
256	1055F953-4640-46EA-82FA-52F6AE2A5589	1C	Windows			10.	2cc38280-a889-4d56-a7ec-56a2aa administrator	LOCALADMIN	FALSE	TRUE	Windows		
257	87F6E8F3-F185-41F4-9C60-0ABB6E3D0D42	1C	Windows Server 2008 R2 Enterprise			10.	2cc38280-a889-4d56-a7ec-56a2aa administrator	LOCALADMIN	FALSE	TRUE	Windows		
258													
259													
260													
	Machines	Users	Services	Groups	Software	Ports	ISAppPools	ScheduledTasks	UsersInGroups				

To save an Excel spreadsheet (.xlsx) copy of the report, click **Save Discovery Report...**, and then select **Save Technical SpreadSheet (.xlsx)**.

To start the process again, click **Start Again**.



IMPORTANT!

When you start again, the current report is not retained. To keep this report, download a copy before starting the process again.



Note: All of the information in the report is **100% private**, and no data is sent back to BeyondTrust or anywhere else.



Note: Credential and Target information is only stored while you use the application. Once the scan is completed and the final report is generated, or when you click **Start Again** or close the application, all credential and target information is deleted.

Configure Windows Hosts for Discovery Scans

Microsoft Windows has several security and configuration settings that affect the ability for vulnerability assessment products to remotely access local resources required for file and registry scanning.

Before making the changes below, verify that your company's security policy allows for this remote access.

To properly scan Windows machines, please check and perform the following:

STEP 1 - Local Security Policy Setting

Set **Network access: Sharing and security model for local accounts** to **Classic**.

For the specified account used when scanning remotely to inherit its local permissions, the local security policy setting must be changed to **Classic** as follows (the same can be changed similarly from the Domain policy):

1. Go to **Control Panel > Administrative Tools > Local Security Settings**.
2. From the left pane, select **Security Settings > Local Policies > Security Options**.
3. From the right pane, scroll down to **Network access: Sharing and security model for local accounts**, and change it to **Classic**. After exiting the Management Console, the setting takes effect immediately.

STEP 2 - Disable (or set exceptions within) Windows Firewall

Allows proper communication between the **Discovery Application** and the target host.

1. Go to **Control Panel > Windows Firewall**.
2. Either **disable** the Windows Firewall or **make exceptions for File and Print Sharing**.



Note: The **Discovery Application** requires that **TCP/445 (Microsoft-DS SMB file sharing)** or **TCP/139 (NetBIOS Session Service)** be **open** on the scan target. These are standard file sharing ports, and are open by default on most versions of Windows. Verify that no in-line devices such as network firewalls are restricting access to these ports.

STEP 3 - Local Security Settings

The local security policy setting **Network access: LAN Manager authentication level** is set to either **all machines set the same** or **Send LM & NTLM - use NTLMv2 session security if negotiated**.

The setting should match what is configured on **Discovery Application**, so that proper authentication protocols are used.

The option is found as follows:

1. Go to **Control Panel > Administrative Tools > Local Security Settings**.
2. From the left pane, select **Security Settings > Local Policies > Security Options**.
3. From the right pane, search for the **Network access: LAN Manager authentication level** setting and compare what is configured on both the *scanner* and *target host*. Testing suggests that the system may require a reboot after making the change, and doesn't necessarily take effect immediately.



Note: Using the **Send LM & NTLM - use NTLMv2 session security if negotiated** option ensures that the scanner can communicate with all NTLM/LM settings, in case Windows workgroup computers ("non domain machines") are not set the same.

STEP 4 - Scanning with an account that is not the built-in administrator or a domain admin

This step is only applicable when scanning Windows targets with an account that is *not* the built-in administrator, but the account is a member of the Local Administrator group.

Windows Vista and later: Starting with Windows Vista, Microsoft introduced *User Account Control (UAC)*. By default, UAC is enabled and can only be disabled from the registry. To deploy **Discovery Application** using credentials other than the built-in *administrator* or *domain administrator* accounts, remote UAC must be *disabled*.



IMPORTANT!

This involves modifying the registry. Please ensure to use the usual precautions about backing it up, prior to proceeding with any registry modifications.

This doesn't apply to domain accounts or the built-in Administrator account. If a domain account is a member of the local Domain Administrators group on the target, the registry setting isn't applicable and full administrator rights are granted for remote requests. To authenticate without UAC remotely, you must set the below registry key to allow this.

Create the following registry *key* and *value*:

1. Press the **Windows key + R**, to access the **Run** dialog box.
2. To start the **Registry Editor**, type **regedit.exe**.
3. Locate the **HKEY_Local_Machine\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system** registry key.
4. In this registry key, create a **LocalAccountTokenFilterPolicy** DWORD value, and set it to **'1': LocalAccountTokenFilterPolicy**.
5. Exit the **Registry Editor**.